TimeCOS 2.5用户手册

北京握奇数据系统有限公司

二000年一月

目　　录

一. TIMECOS简介 5

二. TIMECOS文件组织 8

1. 文件逻辑结构 8

2. 文件空间结构 10

3. 文件访问方式 11

4. 文件类型及命令集 13

5. 文件标识符与文件名称 14

三. TIMECOS独特的安全体系 15

1. 安全状态 15

2. 安全属性 15

3. 安全机制 16

4. 密码算法 17

5. 密钥管理机制 18

四. TIMECOS复位应答 19

五. 命令与应答 21

1. 命令与应答结构 21

2. 状态字SW1 SW2意义 22

六. TIMECOS基本命令 24

1. 增加记录（APPEND RECORD） 24

2. 验证口令(VERIFY PIN) 27

3. 外部认证（EXTERNAL AUTHENTICATE） 30

控制性文档
握奇智能

4. 取随机数 (GET CHALLENGE)..... 32
5. 内部认证(INTERNAL AUTHENTICATE)..... 33
6. 选择文件(SELECT FILE)..... 35
7. 读二进制文件(READ BINARY)..... 39
8. 读记录文件(READ RECORD)..... 42
9. 取响应数据GET RESPONSE(仅用于T=0协议)..... 45
10. 写二进制文件(UPDATE BINARY)..... 47
11. 写记录文件UPDATE RECORD..... 49
12. 解锁口令(UNBLOCK)..... 52
13. 擦除目录文件DF （ERASE DF）..... 54
14. 设置通讯协议（SET PROTOCOL）..... 56
15. 扣款（DECREASE）..... 58
16. 存款（INCREASE）..... 61
17. 数字签名（DIGITAL SIGNATURES）..... 64
18. 签名认证（SIGNATURES VERIFY）..... 66
19. FAC数据加密（DATA ENCRYPT）..... 68
20. FAC数据解密（DATA DECRYPT）..... 70
21. 数据压缩（DATA COMPRESS）..... 72
22. 增加或修改密钥（WRITE KEY）..... 74
23. 建立文件（CREATE FILE）..... 78
24. 验证并修改口令（VERIFY&CHANGE PIN）..... 81
七. 中国金融IC卡专用命令..... 83
1. 卡片锁定（CARD BLOCK）..... 83

控制性文档
握奇智能

2. 应用解锁（APPLICATION UNBLOCK） 85
3. 应用锁定（APPLICATION BLOCK） 87
4. 口令密钥解锁（PIN UNBLOCK） 89
5. 重装/修改口令密钥（RELOAD/CHANGE PIN） 91
6. 圈存（CREDIT FOR LOAD） 93
7. 消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW） 98
8. 圈提（DEBIT FOR UNLOAD） 103
9. 修改透支限额（UPDATE OUVERDRAW LIMIT） 108
10. 取交易认证码（GET TRANSACTION PROVE） 113
11. 读取余额（GET BALANCE） 115
八. 安全报文传送 117
1. 安全报文传送 117
2. 如何实现安全报文传送 117
3. MAC的计算 118
4. 数据加密/解密的计算 120
5. 安全报文传送的命令情况 122
附录一 TIMECOS 2.5金融IC卡应用举例 124
附录二 TIMECOS 2.5安全管理 129
附录三 TIMECOS技术性能指标 131
一. 硬件技术性能参数 131
二. TimeCOS技术性能参数 132

控制性文档
握奇智能

一. TimeCOS简介

由于CPU卡具有很高的安全性及一卡多用的特点，所以IC卡家族中的CPU卡的使用范围正日益扩大。类似一台计算机，CPU卡内也有CPU、存储器和输入、输出接口，所以在应用中CPU卡也必然需要操作系统。北京握奇数据系统有限公司在开发IC卡机具、IC卡终端、IC卡应用软件过程中，积累了丰富的CPU卡操作系统的经验。经过几年的艰苦努力，我公司成功地开发了自主版权的CPU卡操作系统—TimeCOS（Time Card Operating System），该操作系统符合ISO 7816系列标准及<<中国金融集成电路(IC)卡规范>>，适用于保险、医疗保健、社会保障、公共事业收费、安全控制、税务、证件、交通运输、终端安全模块等诸多应用领域,特别是在金融领域，TimeCOS详细规定了电子钱包、电子存折和磁条卡功能（Easy Entry）三种基本应用。

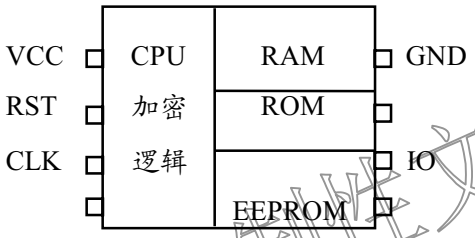
控制性文档
指令集

TimeCOS具有以下特点:

- 支持非对称密码算法:
  支持有限自动机公开钥密码算法(FAC)，实现数字签名与签名认证、数据加密与解密。
- 支持Single DES、Triple DES算法:
  可自动根据密钥的长度选择Single DES、Triple DES算法。
- 支持线路加密、线路保护功能:
  防止通信数据被非法窃取或篡改。
- 支持在一张卡上实现多个不同的应用:
  TimeCOS允许在一张卡上建立三级目录。
- 支持电子钱包和电子存折功能:
  TimeCOS支持PBOC电子钱包和电子存折应用。
- 支持多种文件类型:
  包括二进制文件、定长记录文件、变长记录文件、循环文件、钱包文件。
- 支持多种通讯协议:
  支持T=0（字符传送）和T=1（块传送）通讯协议。
- 支持多种通讯速率:
  支持9600bps、19200bps、38400bps、76800bps。
- 支持多种容量选择:
  可选择512、1K、2K、4K、8K和16K字节的EEPROM空间。
- 满足中国人民银行标准:
  符合<<中国金融集成电路(IC)卡规范>>
- 防插拔功能:

交易处理过程中非正常拔出的卡片自动恢复

TimeCOS内部结构:



控制性文档
指尚智能

- CPU及加密逻辑:

  保证EEPROM中数据安全，使外界不能用任何非法手段获取EEPROM中的数据。

- RAM

  TimeCOS工作时存放命令参数、返回结果、安全状态及临时工作密钥的区域。

- ROM

  存放TimeCOS程序的区域。

- EEPROM

  存放用户应用数据区域，TimeCOS将用户数据以文件形式保存在EEPROM中，在满足用户规定的安全条件时，可进行读或写。

TimeCOS由传输管理、文件管理、安全体系、命令解释四个功能模块组成

- 传输管理 按ISO7816-3标准监督卡与终端之间的通信，保证数据正确地传输，防止卡与终端之间通讯数据被非法窃取和篡改。
- 文件管理 将用户数据以文件形式存储在EEPROM中，保证访问文件时快速性和数据安全性。
- 安全体系 安全体系是TimeCOS的核心部分，它涉及到卡的鉴别与核实，对文件访问时的权限控制机制。
- 命令解释 根据接收到的命令检查各项参数是否正确，执行相应的操作。

TimeCOS指令集:

编号	指令名称	CLA	INS	功能描述	兼容性
1	APPEND RECORD	00/04	E2	增加记录	ISO
2	VERIFY	00/04	20	验证口令	ISO&PBOC
3	EXTERNAL AUTHENTICATE	00	82	外部认证	ISO&PBOC
4	GET CHALLENGE	00	84	取随机数	ISO&PBOC
5	INTERNAL AUTHENTICATE	00	88	内部认证	ISO&PBOC
6	SELECT FILE	00	A4	选择文件	ISO&PBOC
7	READ BINARY	00/04	B0	读二进制文件	ISO&PBOC

8	READ RECORD	00/04	B2	读记录文件	ISO&PBOC
9	GET RESPONSE	00	C0	取响应数据	ISO&PBOC
10	UPDATE BINARY	00/04	D6/D0	写二进制文件	ISO&PBOC
11	UPDATE RECORD	00/04	DC/D2	写记录文件	ISO&PBOC
12	CARD BLOCK	84	16	卡片锁定	PBOC
13	APPLICATION UNBLOCK	84	18	应用解锁	PBOC
14	APPLICATION BLOCK	84	1E	应用锁定	PBOC
15	PIN UNBLOCK	80/84	24	个人密码解锁	PBOC
16	INITIALIZE	80	50	初始化交易	PBOC
17	CREDIT FOR LOAD	80	52	圈存	PBOC
18	DEBIT FOR PURCHASE/CASE WITHDRAW/UNLOAD	80	54	消费/取现/圈提	PBOC
19	UPDATE OVERDRAW LIMIT	80	58	修改透支限额	PBOC
20	GET TRANSCATION PROVE	80	5A	取交易认证	PBOC
21	GET BALANCE	80	5C	读余额	PBOC
22	RELOAD/CHANGE PIN	80	5E	重装/修改个人密码	PBOC
23	ERASE DF	80	0E	擦除DF	专有
24	UNBLOCK	80	2C	解锁被锁住口令	专有
25	SET PROTOCOL	80	14	设置卡片通信参数	专有
26	DECREASE	80/84	30	扣款	专有
27	INCREASE	80/84	32	存款	专有
28	DIGITAL SIGNATURES	80	C2	数字签名	专有
29	SIGNATURES VERIFY	80	C4	签名认证	专有
30	DATA ENCRYPT	80	C6	数据加密	专有
31	DATA DECRYPT	80	C8	数据解密	专有
32	COMPRESS	80	CC	数据压缩	专有
33	WRITE KEY	80/84	D4	增加或修改密钥	专有
34	CREATE FILE	80	E0	建立文件	专有

控制性文档 握台智能

二. TimeCOS文件组织

本章介绍TimeCOS的文件系统，包括文件逻辑结构、文件空间结构以及文件的访问方式。

控制性文档
振奇智能

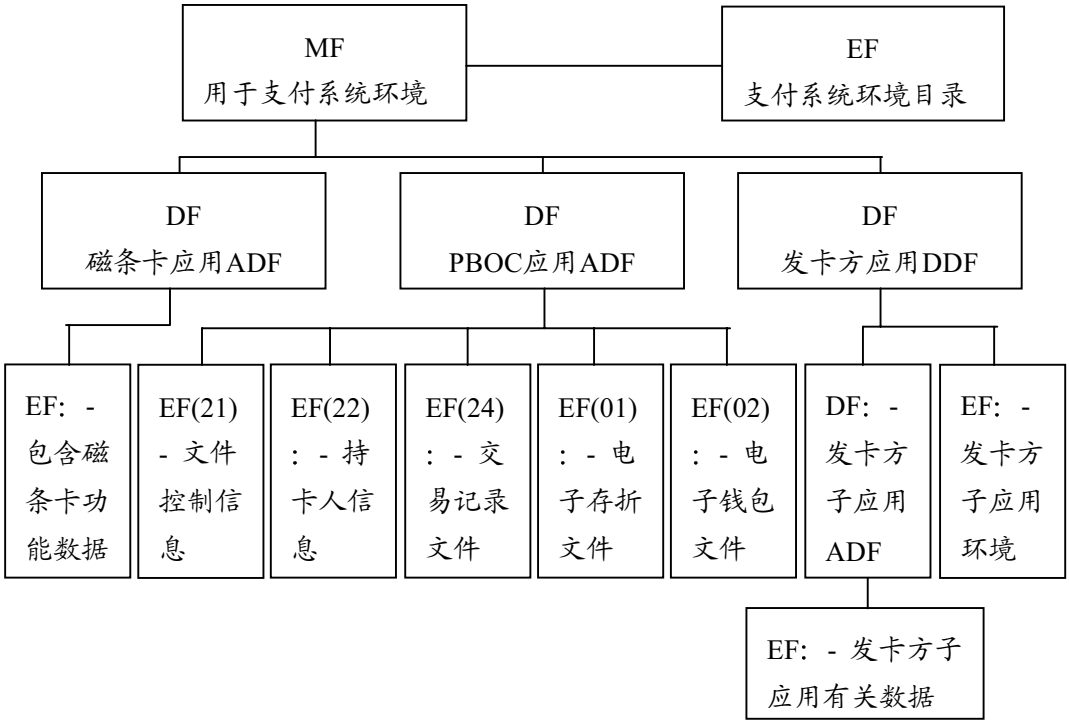
1. 文件逻辑结构

TimeCOS IC卡的基本文件系统是由主文件MF（Master File）、目录文件DF（Directory File）和基本文件EF（Element File）组成。主文件MF在IC卡中唯一存在，在MF下可以有多个目录文件DF和基本文件EF，每一个MF目录下的DF可以存放多个基本文件EF和多个下级目录文件DF，在这里我们称包含下级目录的目录文件为DDF，不含下级目录的目录文件为ADF。

TimeCOS描述了符合<<中国金融集成电路(IC)卡规范>>的应用文件结构，这些应用被定义为支付系统应用。IC卡中支付系统应用可以通过明确选择支付系统环境来激活，一个成功的支付系统环境选择能够对目录结构进行访问。

从终端角度来看，与支付系统应用相关的支付系统环境文件呈一种可通过目录结构访问的树形结构。树的每一分支是一个应用数据文件ADF。一个ADF是一个或多个应用基本文件EF的入口点。一个ADF及其相关数据文件处于树的同一分支上。

下图给出了一个卡片内部结构示例，该卡片支持电子存折、电子钱包、磁条卡功能应用（Easy entry）以及一个没有定义的发卡方应用。



1). MF文件

在TimeCOS卡中，MF文件唯一存在，是卡片文件系统的根。它相当于DOS的根目录。IC卡复位后，卡片自动选择MF文件为当前文件。TimeCOS卡支持用于支付系统环境应用列表的目录结构，支付系统环境由发卡方通过目录选择。目录结构包括一个必备的支付系统目录文件和一些可选的由DDF引用的附加记录。目录文件DF的个数仅受EEPROM空间的限制。

控制性文档
握奇智能

2). DF文件

目录文件DF相当于DOS的子目录，每个DDF下可建立一个目录文件，但不是强制的。任何一个DF在物理上和逻辑上都保持独立，都有自己的安全机制和应用数据，可以通过应用选择实现对其逻辑结构的访问。可以将单个DF文件以及其中一个或多个EF文件当作一个应用，也可以将多个DF以及其中多个EF文件当作一个应用，在使用IC卡时，用户可以根据不同的应用环境自行定义。

3). EF文件

基本文件EF用于存放用户数据或密钥，存放用户数据的文件称为工作基本文件，在满足一定的安全条件下用户可对文件进行相应的操作。存放密钥的文件称为内部基本文件，不可由外界读出，但当获得许可的权限时可在卡内进行相应的密码运算，在满足写的权限时可以修改密钥。

内部基本文件分为KEY文件、FAC秘密钥文件、FAC公开钥文件。

KEY文件必须在MF/DF下最先被建立，且一个目录只能有一个KEY文件，KEY文件可存多个口令密钥、外部认证密钥、DES运算密钥，每个密钥为一条TLV格式的记录。

FAC密钥文件是存放FAC计算所需的公钥或私钥的文件，每个文件只能存放一条公钥或私钥，公钥或私钥在文件中以二进制形式存放。在满足读权限时允许使用READ BINARY命令读出密钥内容，在满足修改权限时可以使用UPDATE BINARY命令进行修改。

工作基本文件可分为二进制文件、定长记录文件，循环文件、钱包文件和变长记录文件。

- 二进制文件： 二进制文件为一个数据单元序列，数据以二进制为单位进行读写，其中的数据结构由应用者解释。
- 定长记录文件：定长记录文件每条记录长度都相同，数据以记录为单位进行存储，记录长度最大为178个字节。
- 循环文件： 循环文件为具有固定长度记录的环行文件，每条记录都只有一个数据域，记录长度最大为178个字节。应用时只能顺序增加记录， 当写记录时，当前写入的为第一条记录，则上一次写入的记录为第二条，依此类推，滚动写入。记录只能在文件头中所规定的范围内滚动写入，当写完最后一条记录时将覆盖最先写入的记录。

- 钱包文件：钱包文件的结构同循环文件，每条记录均为数值型，存款扣款时用记录号1的数值加上或减去该数值，然后将结果存入下条记录中，并将新写的记录作为记录号1。（记录内容高字节在先）

  在MF文件下或DF文件下，可以建立多个钱包文件。在卡片中电子钱包的增额和减额分别受不同安全机制的控制，且在交易、认证过程中采用双卡机制，故大大增强了交易的安全性、独立性、可靠性和保密性。

  普通钱包文件的记录长度必须小于8字节，可使用DECREASE, INCREASE命令对其进行操作.

- 变长记录文件： 变长记录文件的每条记录长度在写记录时是可变的，数据以记录为单位进行存储。更新记录时，新的记录长度必须与卡中的原有记录长度相同，否则本次更新无效。 记录最大长度不能超过178字节。变长记录格式TLV如下:

TAG：标识	Length：长度	Val：值

控制性文档 指令智能

2. 文件空间结构

每个文件在EEPROM中存放的格式如下:

10字节文件头 （文件类型，文件标识符，文件主体空间大小，权限，校验等）
文件主体

每个基本文件所占的EEPROM空间=文件头10字节+文件主体空间。

定长、普通钱包和循环文件的主体空间=记录个数×(记录长度+1)。

每个DF所占的EEPROM空间=DF头10字节+DF下所有文件的空间和+DF名称长度。

MF的空间=MF头10字节+MF下所有文件空间之和。

MF空间不能超过卡EEPROM空间容量，若建MF空间小于EEPROM空间，则剩余空间不可用。

以下列出TimeCOS卡片在部分硬件芯片上的总的可用空间，供参考:

IC卡硬件类型	最大可用空间	建MF命令中的最大主体空间
22C05 (512byte)	477字节	467字节 (01D3H)
44C10 (1K)	987字节	979字节 (03D3H)
44C20 (2K)	2013字节	2003字节 (07D3H)

44C40 (4K)	4061字节	4051字节 (0FD3H)
44C80 (8K)	8157字节	8147字节 (1FD3H)
44C160 (16K)	16349字节	16339字节 (3FD3H)

3. 文件访问方式

控制性文档
握奇智能

- 主文件MF:

  复位后自动被选择，在任何一级子目录下可通过文件标识3F 00或1PAY.SYS.DDF01来选择MF。

- 目录文件DF

  通过文件标识符或目录名称选择目录文件DF。

- 二进制文件

  在满足读条件时可使用READ BINARY读取，在满足写条件时UPDATE BINARY更改二进制文件内容。

- 定长记录文件

  在满足读条件时可使用READ RECORD读指定记录，在满足写条件时使用UPDATE RECORD更改指定记录。

- 循环文件

  在满足读条件时可使用READ RECORD读指定记录，在满足追加条件时可使用APPEND RECORD在文件末尾追加一条记录，当记录写满后自动覆盖最早写的记录，最后一次写入的记录，其记录号总是1，上次写入的记录号是2，依次类推。

- 钱包文件

  对于普通钱包文件：在满足扣款条件时可使用DECREASE扣款，使用READ RECORD读出余额，在满足存款条件时可以使用INCREASE追加余额。

  对于记录长度等于8字节的钱包文件：在满足使用条件时可用READ RECORD读出整条记录或用GET BALANCE读余额或在规定的密钥控制下完成圈存、圈提、消费、取现、修改透支限额。

- 变长记录文件

  在满足读条件时可使用READ RECORD读出指定记录，在满足写条件时可以使用UPDATE RECORD写一条新记录或更改已存在的记录，或用APPEND RECORD在文件末尾追加一条新记录。变长记录文件的格式为TLV格式，Tag为1字节记录标识，L为一字节记录数据域长度。V为L字节数据值。在执行UPDATE RECORD更改已存在的记录时，新写的整条记录长度必须和原来的整个记录长度相等，否则该命令不能成功执行。

- FAC秘密钥文件

在满足使用条件时可执行数字签名、解密，在满足读权限时可用READ BINARY命令读出密钥内容，在满足写的条件时可用UPDATE BINARY来修改文件内容。

- FAC公开钥文件

在满足使用条件时可执行签名认证、加密，在满足读权限时可用READ BINARY命令读出密钥内容，在满足写的条件时可用UPDATE BINARY来修改文件内容。

- KEY文件及其文件中的密钥：

每个DF或MF下只能有一个KEY文件，且必须最先被建立，在任何情况下密钥数据均无法读出。当进入DF或MF时，若该目录下无KEY文件和其它文件，则在该目录下可任意建立文件和读写文件而不受文件访问权限的限制。一旦离开该目录再进入此目录时，将遵循文件的访问权限。

在KEY文件中可以存放多个密钥，每个密钥为一条可变长的记录，记录的长度为密钥数据长度加7。如Triple DES密钥记录的长度为23字节，Single DES密钥记录的长度为15字节。

在满足KEY文件增加密钥的权限时可用WRITE KEY增加一条密钥记录，在满足某个密钥规定的更改权限时可使用WRITE KEY更改密钥数据，在满足使用权限时才可使用相应的密钥进行认证或密码运算。

密钥具有独立性，用于一种特定功能的加密/解密密钥不能被任何其它功能所使用，包括保存在IC卡中的密钥和用来产生、派生、传输这些密钥的密钥。

口令密钥：

在满足口令密钥的使用权限时，可用VERIFY核对口令，或PIN CHANGE/UNBLOCK更改并解锁口令.在核对口令通过之后，设置安全状态寄存器的值为该口令密钥规定的后续状态值。口令密钥中提供错误次数计数器，每次核对口令失败时错误次数计数器自动减一，当错误次数达到0时，口令密钥被自动锁住。

解锁口令密钥：

在满足使用权限时，可通过UNBLOCK核对解锁口令而达到解锁因连续核对口令错误被封锁的口令密钥，同时修改新的口令。解锁口令锁死后无法再被解锁。

外部认证密钥：

在满足使用权限时可执行EXTERNAL AUTHENTICATE命令进行外部认证，在满足更改权限时可使用WRITE KEY更改密钥。外部认证密钥锁死后无法被解锁。

DES运算密钥：

控制性文档 握奇智能

DES运算密钥又分为DES加密密钥、DES解密密钥和MAC密钥。在满足使用权限时可执行加密、解密或生成MAC运算，在满足更改权限时可用WRITE　KEY来修改密钥的内容。

4.　文件类型及命令集

下表为TimeCOS命令适用的文件类型及命令集，水平方向表示TimeCOS的文件类型， 垂直方向表示TimeCOS命令集:

文件类型 / 命令	MF 38	DF 38	二进制 28	定长记录 2A	循环 2E	钱包 2F	变长记录 2C	秘密密钥文件 3D	公开密钥文件 3E	KEY文件 3F
CREATE	V	V	V	V	V	V	V	V	V	V
SELECT	V	V	V	V	V	V	V	V	V	V
READ BINARY			V							
UPDATE BINARY			V					V	V	
READ RECORD				V	V	V	V			
UPDATE RECORD				V			V			
APPEND RECORD					V		V			
DECREASE						V				
INCREASE						V				
DIGITAL SIGNATURES								V		
SIGNATURES VERIFY									V	
DATA ENCRYPT									V	
DATA DECRYPT								V		
WRITE　KEY										V
ERASE　DF	V	V								
CREDIT FOR LOAD						V				
DEBIT FOR PURCHASE/CASE WITHDRAW						V				
DEBIT FOR UNLOAD						V				
GET BALANCE						V				
GET TRANSCATION PROVE						V				
INITIALIZE FOR CASE WITHDRAW						V				
INITIALIZE FOR LOAD						V				
INITIALIZE FOR PURCHASE						V				
INITIALIZE FOR UNLOAD						V				
INITIALIZE FOR UPDATE						V				
UPDATE OVERDRAW LIMIT						V				

说明:

控制性文档 握奇智能

表格中V表示命令可用于对应的文件类型，如第三行第三列为V表示用READ BINARY命令可读二进制文件，第三行第四列无V标识，表示定长记录文件不可用READ BINARY命令读取。

文件类型表示文件内部结构组织形式，用一个字节来表示，如某个文件类型为28H则表示该文件为二进制文件。文件类型在建立文件时规定。

控制性文档
握奇智能

5. 文件标识符与文件名称

文件标识符是文件的标识代码，用2个字节来表示，在选择文件时只要指出该文件的标识代码，TimeCOS就可以找到相应文件，同一目录下的文件标识符必须是唯一的。MF的文件标识符是3F00，文件名为1PAY.SYS.DDF01。

所有文件都可以通过文件标识符用SELECT命令进行选择，目录文件DF还可以通过目录名称进行选择。

短文件标识符选择可以通过READ BINARY、UPDATE BINARY命令的参数P1来实现文件的选择：若参数P1的高三位为100，则低5位为短的文件标识符。eg. 若P1为81H即10000001，其中高三位为100，则所选的文件标识符为0001。

短文件标识符选择还可以通过READ RECORD、UPDATE RECORD、APPEND RECORD、DECREASE、INCREASE命令的参数P2来实现文件的选择：若P2的高五位不全为0，低三位为100，则高五位为短的文件标识符。eg. 若P2为0CH即00001100，其中低三位为100，所选的文件标识符为0001。

短文件标识符选择只能用五位来决定文件标识符，所以可选择的最大文件标识符为31。若文件需要用短文件标识符进行选择，则建立文件时就需将文件标识符取在1-31（00001-11111）之间。

选择文件后，只要文件存在，该文件就被置为当前文件，以后可以不用选择而直接对该当前文件进行操作。

三. TimeCOS独特的安全体系

TimeCOS的安全体系从念上可以分为安全状态、安全属性、安全机制、密码算法和密钥管理机制。

控制性文档
握奇智能

1. 安全状态

安全状态是指卡在当前所处的一种安全级别。TimeCOS的根目录和应用目录分别具有16种不同的安全状态。TimeCOS在卡内部用两个4位寄存器来表示安全状态：一个寄存器称为MF的安全状态寄存器，它表示整个卡所处的安全级别；另一个寄存器为当前目录的安全状态寄存器，每个寄存器的值可以是0至F之间的某一值。

MF的安全状态寄存器的值复位后为0，应用目录的改变不会影响该寄存器的值，只有MF下的口令核对或外部认证通过后MF的安全状态寄存器值才发生变化。

当前目录的安全状态寄存器的值在复位后或选择目录文件命令成功地被执行时被置为0，如选择下级子目录时被置为0，在当前目录下的口令核对或外部认证通过后该状态寄存器值发生变化。若在当前目录下的核对口令或外部认证命令返回的错误状态为63Cx,则该安全状态寄存器被置为0.

若当前目录为MF，则当前目录的安全状态寄存器的值等于MF的安全状态寄存器值。

2. 安全属性

安全属性是指对某个文件进行某种操作时所必须满足的条件，也就是在进行某种操作时要求安全状态寄存器的值是什么。

安全属性又称访问权限，一种访问权限在建立该文件时用一个字节指定。TimeCOS的访问权限有别于其它任何操作系统的访问权限，它用一个区间来严格限制其他非法访问者。

访问权限为0Y时表示要求MF的安全状态寄存器的值大于等于Y。如某文件读的权限为05表示在对该文件进行读之前必须使MF的安全状态寄存器的值大于等于5。

访问权限为XY时（X不为0）表示要求当前目录的安全状态寄存器的值大于等于Y且小于等于X。若X=Y表示要求当前目录的安全状态寄存器的值等于X，若X<Y表示不允许该操作。 如某文件写的权限为53表示对该文件进行写之前必须使当前目录的安全状态寄存器的值为3、4或5。

例：某文件读的权限为F0，写的权限为F1，代表可任意读取，写时必须满足当前目录的安全

状态寄存器的值大于等于1。

3. 安全机制

安全机制是指某种安全状态转移为另一种安全状态所采用的方法和手段。TimeCOS通过核对口令和外部认证来改变安全状态寄存器的值。当在MF下时，认证通过之后同时改变MF和当前目录的安全状态寄存器的值，若不在MF下则认证通过之后只改变当前目录的安全状态寄存器值。

当建立口令或外部认证密钥时，参数的后续状态表示该口令核对成功或外部认证成功后，置当前目录的安全状态寄存器的值为后续状态。如某口令密钥的后续状态为01表示对口令核对成功后，当前目录的安全状态寄存器的值为1。当上电复位后或从父目录进入子目录或退回上级目录时，当前目录的安全状态寄存器的值均自动被置为0。

为更好的理解TimeCOS的安全机制，下面举一例说明:

设卡中某目录下有一个二进制文件，定义读二进制文件的权限为F1,写二进制文件权限为F2。该目录下有一个口令密钥，口令核对通过之后的后续状态为1，卡中有一外部认证密钥，使用权限为11，外部认证通过之后后续状态为2。

请看下面的操作及当前目录的状态寄存器的变化情况:

卡终端操作	当前目录安全状态寄存器的值
选择该目录 →	0
(不是MF) ←	送返回信息
读二进制 →	0
←	读的权限不满足，不允许读
验证口令 →	1
←	口令核对正确
读二进制 →	1
←	送出读出的数据
写二进制 →	1
←	写的权限不满足，不允许写
外部认证 →	2
←	外部认证正确
写二进制 →	2
←	写成功
读二进制 →	2
←	送出读出的数据

4. 密码算法

TimeCOS 2.5支持Single DES、Triple DES、FAC公开钥密码算法。

在建立DES密钥时，若密钥长度为8字节则运算时使用Single DES算法，若密钥长度为16字节则运算时使用Triple DES算法(MAC只能用Single DES算法)。

运算时使用加密还是解密算法完全由密钥类型决定，如：用于加密的密钥不可用于解密或MAC运算，用于外部认证的密钥也不可用于内部认证。

TimeCOS在使用DES算法时，若数据长度大于8字节时使用ECB模式，若数据长度不是8的倍数时在计算过程中自动在数据后补80 00...00使其长度为8的倍数。如果数据为12 23 34 56 78 89 90 A1 B1，由于数据长度不是8的倍数，所以在计算过程中自动将数据改写为12 23 34 56 78 89 90 A1 B1 80 00 00 00 00 00 00 00后再进行计算。

用DES算法作外部认证的过程如下:

卡终端	TimeCOS卡
取随即数 →	
	← 送随机数
卡终端用密钥加密该随机数	
送卡作外部认证 →	卡用相同密钥解密并与送出的随机数比较
	← 送比较结果，并置安全状态寄存器值为该密钥后续状态。

非对称密码算法:

非对称密码体制又称公开钥密码体制，加密和解密分别通过两个不同的密钥来实现，需要保密的密钥称为秘密钥，对应的另一个密钥称为公开钥，无需保密，企图由公开钥推导出秘密钥是不可行的。

有限自动机公开钥密码体制(FAC)是第一个“时序型”的公开钥密码体制，其安全性建立在非线性有限自动机求逆和矩阵多项式分解的困难之上，该体制可实现加密、解密、数字签名、签名认证。

用公开钥密码体制实现卡认证及交易过程如下:

1. 发卡中心生成一对密钥(PKU SKU)，将PKU保存到卡终端中。
2. 为用户生成一对密钥(PKC SKC)，秘密钥存到用户卡中，将卡号及公钥PKC用SKU进

控制性文档 振奇智能

行签字，然后存到卡中和发卡中心主机系统中。

3. 应用时卡终端读出卡号、公钥PKC及其签字，用终端中的PKU进行验证。
4. 卡终端将交易送用户卡中SKC签字。
5. 卡终端对签字进行验证并将交易数据及用户卡签字保存到卡终端中。

5. 密钥管理机制

控制性文档
振芯智能

TimeCOS密钥管理机制符合中国人民银行PSAM卡标准，密钥的装载、更新和下发都有一整套安全的管理办法。

TimeCOS的密钥安装可以明文或密文安装，如采用密文安装方式，则密钥的安装是在应用主控密钥KActl（即当前应用下的密钥标识为00的外部认证密钥）的控制下进行装载的。

例如：密文且带MAC方式装载某一16字节密钥:

1、 使用应用主控密钥对下列数据进行加密：Data = ‘15’ （以下数据的长度）||密钥属性（5字节，其中密钥类型字节的高半字节为 ‘F’ ）||密钥明文（16字节），记为C = 3DES（KActl，Data）（ ‘18’ 字节）

2、 使用应用主控密钥对下列数据进行MAC运算：Data = ‘84’ ‖ ‘D4’ ‖ ‘01’ ||KID|| ‘1C’ ||C（ ‘18’ 字节），记为M = MAC（KActl，Data）（4字节）

3、 命令报文如下： ‘84’ ‖ ‘D4’ ‖ ‘01’ ||KID|| ‘1C’ ||C（ ‘18’ 字节）||M（4字节）。

TimeCOS密钥的更新机制可以采用密文方式，密钥更新时，判断该密钥属性是否需要采用密文方式，如需要，则在应用主控密钥的控制下更新。

例如：密文带MAC更新上述例子的密钥:

1、使用应用主控密钥对下列数据进行加密：Data = ‘10’ （以下数据的长度）||密钥新明文（16字节），记为C = 3DES（KActl，Data）（ ‘18’ 字节）

2、使用应用主控密钥对下列数据进行MAC运算：Data = ‘84’ ‖ ‘D4’ ||密钥类型（ ‘3x’ ）||KID|| ‘1C’ ||C（ ‘18’ 字节），记为M = MAC（KActl，Data）（4字节）

3、命令报文如下： ‘84’ ‖ ‘D4’ ||密钥类型（ ‘3x’ ）||KID|| ‘1C’ ||C（ ‘18’ 字节）||M（4字节）。

四．TimeCOS复位应答

对于T=0通讯协议的卡，复位应答信息如下:

符号	值	说　明
TS	3B	正向约定，首先传送的是字符最低有效位
T0	69	TB和TC1存在，历史字符为9个
TB1	00	无需额外编程电压VPP
TC1	00	无需额外的保护时间
T_1—T_9	XX	历史字符

注：对TimeCOS卡复位时，返回的第一个字节TS的值均为3B，它表示从IO口传送数据时先传低位再传高位。返回的第二个字节为T0，它的低半字节表明可选历史字符的数目（0到15），高半字节表示后续字符TA1到TD1是否存在，逻辑1表明相应字符存在。

如上图所示，69：9表示后面有9个字节的历史数据。

6(0110) 表示TB1、TC1存在，由于TD1不存在所以为T=0的通讯协议。

由于在T=0情况下使用指令比较麻烦，大多数情况下采用T=1的通讯协议。

对于T=1通讯协议的卡，复位应答信息如下:

符号	值	说明
TS	3B	正向约定，首先传送的是字符最低有效位
T0	E9	TB1、TC1和TD1存在，历史字节9个
TB1	00	无需额外的编程电压VPP
TC1	00	两个字符之间延时减少到11个etu
TD1	81	TA2到TC2不存在，TD2存在，使用T=1通讯协议
TD2	31	TA3和TB3存在，TC3和TD3不存在，使用T=1通讯协议
TA3	B7	一次最多可传送183个字符
TB3	45	BWI=4，CWI=5
T_1—T_9	XX	历史字符
TCK	XX	校验字符

注：如上图所示，E9:　　9表示后面有9个字节的历史数据。

E(1110) 表示TB1、TC1、TD1存在。TD1的值为81，低半字节为1表示后续信息交换使用T=1的通讯协议，高半字节表示TA2到TD2是否存在。

历史字符如下:

符号	值	意　义
T_1	XX	TimeCOS版本号
T_2—T_9	XX	8字节卡序号，每卡该序号唯一

注：TCK具有一个校验复位应答期间所发送数据完整性的值。TCK的值应使从T0到包括TCK在内的所有字节进行异或运算而结果为00。

在使用T=0协议时，IC卡不回送TCK。

恒宝股份 证券代码：002104 恒宝智能 深圳证券交易所 公开披露文档

五. 命令与应答

1. 命令与应答结构

控制性文档
握奇智能

- 情形一:

命令:

CLA	INS	P_1	P_2	00

应答:

SW1	SW2

- 情形二:

命令:

CLA	INS	P_1	P_2	Le

应答:

Le字节DATA	SW1	SW2

- 情形三:

命令:

CLA	INS	P_1	P_2	Lc	DATA

应答:

SW1	SW2

- 情形四:

命令:

CLA	INS	P_1	P_2	Lc	DATA	Le

应答:

Le字节DATA	SW1	SW2

CLA
指令类别

INS
指令类型的指令码，见一，TimeCOS简介

P1 P2
命令参数

Lc
数据域DATA长度，该长度不可超过178字节

DATA
数据域或应答数据域

Le

要求返回数据长度，Le为00表示返回卡中最大数据长度，该长度不可超过178字节

SW1 SW2

卡执行命令的返回代码（状态字）。

2. 状态字SW1 SW2意义

任意一条命令的应答至少由一个状态字（2个字节）组成。状态字说明了命令处理的情况，即命令是否被正确执行，如果未被正确执行，原因是什么。

控制性文档
指南智能

SW1 SW2	意　　义
90 00	正确执行
62 81	回送的数据可能错误
62 83	选择文件无效，文件或密钥校验错误
63 CX	X表示还可再试次数
64 00	状态标志未改变
65 81	写EEPROM不成功
67 00	错误的长度
69 00	CLA与线路保护要求不匹配
69 01	无效的状态
69 81	命令与文件结构不相容
69 82	不满足安全状态
69 83	密钥被锁死
69 85	使用条件不满足
69 87	无安全报文
69 88	安全报文数据项不正确
6A 80	数据域参数错误
6A 81	功能不支持或卡中无MF或卡片已锁定
6A 82	文件未找到
6A 83	记录未找到
6A 84	文件无足够空间
6A 86	参数P1 P2错误
6B 00	在达到Le/Lc字节之前文件结束，偏移量错误
6C xx	Le错误

6E 00	无效的CLA
6F 00	数据无效
93 02	MAC错误
93 03	应用已被锁定
94 01	金额不足
94 03	密钥未找到
94 06	所需的MAC不可用

控制性文档
指令智能

注：当SW1的高半字节为‘9’，且低半字节不为‘0’时，其含义依赖于相关应用。

当SW1的高半字节为‘6’，且低半字节不为‘0’时，其含义与应用无关。

六. TimeCOS基本命令

控制性文档
握奇智能

1. 增加记录（APPEND RECORD）

1). 定义和范围

APPEND RECORD命令用于对变长记录文件、循环文件追加记录。

2). 命令报文

APPEND RECORD命令报文编码如下:

代码	值
CLA	00/04
INS	E2
P1	00
P2	见表1
Lc	XX
Data	写入的数据
Le	不存在

表1: 参数P2的含义

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X	0	0	0	b4-b8为短文件标识符
0	0	0	0	0	0	0	0	当前文件

Lc表示要写入的字节数。

1. 若为线路保护，Lc为写入数据的长度+4字节MAC。
2. 若为加密线路保护，Lc为加密后数据的长度+4字节MAC。

对循环文件若记录已满则覆盖最早写入的记录，且新增加记录的记录号总为1。

3). 命令报文数据域

命令报文数据域由追加记录组成。

若为线路保护则由追加记录附上4字节MAC码组成。

若为线路加密保护则由被加过密的记录数据附上4字节MAC码组成。

控制性文档
握奇智能

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC可能回送的错误如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
65 81	写EEPROM失败
67 00	长度错误(Lc域为空)
69 81	当前文件不是循环文件或变长记录文件
69 82	不满足安全状态
6A 81	不支持此功能（无MF或MF已锁定）
6A 82	未找到文件
6A 83	未找到记录
6A 84	文件中存储空间不够（对变长记录文件）

6). 举例说明

- CASE1：对变长记录文件追加记录

[例1]：文件标识符为0001的变长记录文件，建立时不采用线路保护。

往变长记录文件中增加1条记录标识为AA的记录，不进行线路保护，则命令为:

00 E2 00 08 0E AA 0C 11 22 33 44 55 66 77 88 99 AA BB CC

[例2]：文件标识符为0002的变长记录文件，建立时采用了线路保护。

往变长记录文件中增加1条记录标识为BB的记录，必须使用线路保护密钥进行线路保护，则命令为:

04 E2 00 10 0A BB 04 11 22 33 44 60 23 3C 19

说明：BB 04 11 22 33 44为写入的数据，60 23 3C 19为使用线路保护密钥生成的4字节的

MAC。

[例 3]：文件标识符为0003的变长记录文件，建立时采用了线路加密保护。

往变长记录文件中增加1条记录标识为CC的记录，必须使用线路保护密钥进行线路加密保护，则命令为：04 E2 00 18 0C BD B7 DB 2A 99 51 17 5C EF 56 55 26

说明：BD B7 DB 2A 99 51 17 5C为使用线路保护密钥对数据CC 04 01 02 03 04加密后的结果，EF 56 55 26为使用线路保护密钥生成的4字节MAC。

- CASE2：对循环文件追加记录

[例1]：文件标识符为0001的循环文件，它有2条记录，每条记录长度为6个字节，建立时不采用线路保护。

如该文件为当前文件，往循环文件中追加1条记录，不进行线路保护，则命令为：00 E2 00 00 06 11 22 33 44 55 66

[例2]：文件标识符为0003的循环文件，它有2条记录，每条记录长度为8个字节，建立时采用线路保护。

往循环文件中追加1条记录，必须使用线路保护密钥进行线路保护，则命令为：04 E2 00 18 0C 01 02 03 04 05 06 07 08 31 E1 D4 F7

说明：01 02 03 04 05 06 07 08为写入的数据，31 E1 D4 F7为使用线路保护密钥生成的4字节MAC。

[例3]：文件标识符为0001的循环文件，它有2条记录，每条记录长度为7个字节，建立时采用线路加密保护。

往循环文件中追加1条记录，必须使用线路保护密钥进行线路加密保护，则命令为：

04 E2 00 08 0C D8 E9 A7 D9 9F 15 87 82 57 8A AC A8

说明：D8 E9 A7 D9 9F 15 87 82为使用线路保护密钥对数据11 22 33 44 55 66 77加密后的结果，57 8A AC A8为使用线路保护密钥生成的4字节MAC。

[注]:此处用到的线路保护密钥为线路保护密钥.

非制性文档
握奇智能

2. 验证口令(VERIFY PIN)

1). 定义与范围

VERIFY PIN命令用于校验命令数据域的口令密钥的正确性。

控制性文档
握奇智能

2). 命令报文

VERIFY PIN命令的编码如下:

代码	值
CLA	00/04
INS	20
P1	00
P2	口令密钥标识号
Lc	02-08
Data	外部输入的口令密钥
Le	不存在

在满足该口令密钥文件使用权限时才可执行该命令。

若口令验证成功，则安全状态寄存器的值被置成该密钥的后续状态，同时口令错误计数器被置成初始值。

若验证错误，则口令可试次数减一，若口令已被锁死，则不能再执行该命令，但当口令长度为8字节时，可用解锁口令对其进行解锁，使原口令密钥文件恢复正常，同时口令错误计数器被恢复成初始值。若口令长度为02-06字节时,可以用PBOC_IC命令对其进行解锁,重装等操作,并可能成功地返回9000.

[说明]: 若PIN值的后面字节为连续的FF,校验时可以忽略该段字节,但若PIN值为全FF,则最少应输入一个FF值.

3). 命令报文数据域

命令报文数据域由持卡者输入的口令密钥组成。

若为线路保护则由口令密钥附上4字节MAC码组成。

若为线路加密保护则由被加过密的口令密钥附上4字节MAC码组成。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

当前的应用选择中，命令数据域中外部输入的口令密钥与卡中存放的口令密钥校验失败时，IC卡将回送SW2=Cx，x表示个人密码允许重试的次数：当卡回送C0时，表示不能重试口令密钥。此时再使用VERIFY PIN命令时，将回送失败状态码SW1 SW2= ‘6983’。

IC卡可能回送的状态码如下所示：

SW1 SW2	意　　义
90 00	命令成功执行
63 Cx	还剩x次可试机会
62 83	口令密钥校验错误
67 00	错误的长度
69 81	不是口令密钥
69 82	密钥使用条件不满足
69 83	认证方法（口令密钥）锁死
6A 82	KEY文件未找到
93 02	密钥线路保护错误
94 03	密钥未找到

[例1]：密钥标识号为01的口令密钥，使用权F0，错误计数器33，后续状态11，7字节的个人密码为31 32 33 34 35 36 37，建立时不采用线路保护。

验证口令，不进行线路保护，则命令为：

00 20 00 01 07 31 32 33 34 35 36 37

[例2]：密钥标识号为01的口令密钥，使用权F0，错误计数器33，后续状态11，7字节的个人密码为31 32 33 34 35 36 37，建立时采用线路保护。

验证口令，使用线路保护密钥进行线路保护，则命令为：

04 20 00 01 0B 31 32 33 34 35 36 37 CE A9 FE C1

说明：CE A9 FE C1为使用线路保护密钥生成的4字节MAC码。

[例3]：密钥标识号为01的口令密钥，使用权F0，错误计数器33，后续状态11，7字节的个

深圳性文档 指令智能

人密码为31 32 33 34 35 36 37，建立时采用线路加密保护。

验证口令，使用线路保护密钥进行线路加密保护，则命令为：

04 20 00 01 0C 7E 05 8B 7C 2F C6 E2 B3 6A 1A AC C7

说明：7E 05 8B 7C 2F C6 E2 B3为使用线路保护密钥对7字节个人密码31 32 33 34 35 36 37加密后的结果，6A 1A AC C7为使用线路保护密钥生成的4字节MAC码。

[注]: 该命令使用的线路保护密钥为口令解锁密钥.

控制性文档
握奇智能

3. 外部认证（EXTERNAL AUTHENTICATE）

1). 定义和范围

EXTERNAL AUTHENTICION命令要求IC卡中存在用于外部认证的密钥。

在满足该密钥的使用条件且该密钥未被锁死时才能执行此命令。

将命令中的数据用指定外部认证密钥解密，然后与先前产生的随机数进行比较，若一致则表示认证通过，置安全状态寄存器为该密钥规定的后续状态值，错误计数器恢复成初始值；若比较不一致则认证失败，可再试错误数减一，且不改变安全状态寄存器的值。

2). 命令报文

EXTERNAL AUTHENTICATE命令报文编码如下:

代码	值
CLA	00
INS	82
P1	00
P2	外部认证密钥标识号
Lc	08
Data	8字节加密后的随机数
Le	不存在

3). 命令报文数据域

命令报文数据域中包括8字节加密后的随机数。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
63 Cx	还剩x次可试机会
67 00	错误的长度
69 81	不是外部认证密钥
69 82	密钥使用条件不满足
69 83	认证方法（外部认证密钥）锁死
6A 82	KEY文件未找到
93 02	安全信息不正确
94 03	密钥未找到

深圳市文档
接口智能

[例]：密钥标识号为01的外部认证密钥，使用权F0，更改权EF，错误计数器33，后续状态01，8字节的密钥为01 02 03 04 05 06 07 08，则外部认证的过程如下：

卡终端	TimeCOS卡
取随机数 →	
←	送随机数
卡终端用密钥加密该随机数	
送卡作外部认证 →	卡用相同密钥解密并与送出的随机数比较
←	送比较结果，并置安全状态寄存器值为该密钥后续状态。

1. 卡终端从TimeCOS卡取随机数，则命令为：

   00 84 00 00 08

   由卡片返回的响应数据为：BB 83 BF F3 D9 9F 31 62 9000

   说明：BB 83 BF F3 D9 9F 31 62为卡片返回的8字节的随机数。

2. 卡终端用与外部认证密钥相同的密钥01 02 03 04 05 06 07 08对随机数进行加密，加密后的结果为：

   63 63 95 34 DB 41 91 99

3. 卡终端将加密后的随机数送到卡中作外部认证，如果成功则置安全状态寄存器值为该外部认证密钥的后续状态01，命令为：

   00 82 00 01 08 63 63 95 34 DB 41 91 99

4. 取随机数 (GET CHALLENGE)

1). 定义和范围

GET CHALLENGE命令请求一个用于线路保护过程的随机数。

由卡产生Le字节随机数送给终端，若下条指令为外部认证，则外部认证数据用指定的外部认证密钥解密后与该随机数进行比较。

控制性文档
握奇智能

2). 命令报文

GET CHALLENGE命令报文编码如下:

代码	值
CLA	00
INS	84
P1	00
P2	00
Lc	不存在
Data	不存在
Le	04-10

3). 命令报文数据域

命令报文数据域不存在

4). 响应报文数据域

响应报文数据域包括随机数，长度为Le个字节。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
6A	81	不支持此功能（无MF或卡片已锁定）
67	00	长度错误

5. 内部认证(INTERNAL AUTHENTICATE)

控制性文档
握奇智能

1). 定义和范围

在满足该密钥的使用条件时才能执行此命令。

INTERNAL AUTHENTICATION命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。

2). 命令报文

INTERNAL AUTHENTICATE命令报文编码如下:

代码	值
CLA	00
INS	88
P1	00/01/02
P2	DES密钥标识号
Lc	认证数据的长度
Data	认证数据
Le	不存在

DES密钥标识：TimeCOS用密钥本身规定的算法进行相应的DES运算。例如密钥类型为30(或31或32)则TimeCOS用密钥文件中的密钥对数据进行加密(或解密或生成MAC)。P1为00时表示加密,01时表示解密,02时表示生成MAC.

3). 命令报文数据域

命令报文数据域的内容是应用专用的认证数据。

4). 响应报文数据域

响应报文数据域的内容是相关认证数据，即DES运算的结果。

5). 响应报文状态码

IC卡可能回送的错误状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
67 00	错误的长度
69 81	密钥与运算方法不匹配
69 82	不满足安全状态
69 85	不满足使用条件
6A 82	KEY文件不存在
94 03	密钥未找到

深圳性文档 握奇智能

[说明]: 如果KEY文件中没有相应类型的密钥，卡片将返回‘9403’即密钥未找到。

[例1]: 密钥标识号为01的DES加密密钥，使用权F0，更改权EF，算法标识00，密钥版本号01，8字节的密钥为11 22 33 44 55 66 77 88，则内部认证即DES加密过程如下:

对数据01 02 03 04 05 06 07 08进行DES加密，则命令为:

00 88 00 01 08 01 02 03 04 05 06 07 08

由卡片返回的响应数据为:

17 8F 59 F8 57 8E 0D 3F 9000

说明: 17 8F 59 F8 57 8E 0D 3F为内部认证即DES加密的结果。

[例2]: 密钥标识号为02的DES解密密钥，使用权F0，更改权EF，算法标识98，密钥版本号05，8字节的密钥为11 22 33 44 55 66 77 88，则内部认证即DES解密过程如下:

对数据17 8F 59 F8 57 8E 0D 3F进行DES解密，则命令为:

00 88 01 02 08 17 8F 59 F8 57 8E 0D 3F

由卡片返回的响应数据为:

01 02 03 04 05 06 07 08 9000

说明: 01 02 03 04 05 06 07 08为内部认证即DES解密的结果。由此可以看出，相同密钥的DES加密过程和DES解密过程互为逆过程。

[例3]: 密钥标识号为03的DES MAC密钥，使用权F0，更改权EF，算法标识98，密钥版本号05，8字节的密钥为11 22 33 44 55 66 77 88，则内部认证即生成MAC过程如下:

对数据01 02 03 04 05 06 07 08进行加密生成MAC，则命令为:

00 88 02 03 08 01 02 03 04 05 06 07 08

由卡片返回的响应数据为:

A8 2A 8C EB 9000

说明: A8 2A 8C EB为通过内部认证生成的4字节的MAC码。

[注]: 内部认证实际上就是DES运算，无论内部认证成功与否均不能改变安全状态寄存器的值。

6. 选择文件(SELECT FILE)

1). 定义和范围

SELECT FILE命令通过文件名、文件标识符或选择下一个应用来选择IC卡中MF、DDF或ADF。从IC卡的响应报文应由回送文件控制信息FCI组成。

控制性文档
握奇智能

2). 命令报文

SELECT命令报文编码如下:

代码	值
CLA	00
INS	A4
P1	00/04
P2	见说明
Lc	XX
Data	文件标识符或DF名称（ ‘05’ ~ ‘10’ 字节）
Le	对于DF而言为FCI的长度

说明:

P1=00 按文件标识符选择（P2必须等于0），选择当前目录下基本文件或子目录文件。

P1=04 用目录名称选择，P2=00表示第一个或仅有一个，P2=02表示下一个。用该方法可以选择DF。

在任何情况下均可通过标识符3F 00或目录名称1PAY.SYS.DDF01选择MF。

3). 命令报文数据域

命令报文数据域可为空或包含文件标识符或DF名称。

4). 响应报文数据域

响应报文数据域应包括所选择的DDF或ADF的文件控制信息(FCI)。见下表:

表1定义了成功选择了DDF后回送的文件控制信息FCI:

标志	值	存在方式
6F	文件控制信息模板	必备
84	DF名	必备
A5	文件控制信息专用数据	必备
88	目录基本文件的短文件标识符	必备

表2定义了成功选择了ADF后回送的文件控制信息FCI:

标志	值	存在方式
6F	文件控制信息模板	必备
84	DF名	必备
A5	文件控制信息专用数据	必备
9F0C	发卡方自定数据的文件控制信息	可选

控制性文档 指南智能

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
67	00	错误的长度
6A	81	不支持此功能(无MF或卡片已锁定)
6A	82	未找到文件
6A	86	参数P1 P2不正确

例：符合银行标准的应用目录的选择

1。建立MF时指定MF下指示目录结构的基本文件(DIR)的短文件标识符为01，对主文件MF进行选择即对DDF进行选择，则命令为:

00 A4 00 00 02 3F 00

由卡片返回的响应数据为:

6F 15 84 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 A5 03 88 01 01 9000

说明：返回的信息为嵌套的TLV格式的变长记录。‘6F’为文件控制信息模板的记录标识，‘15’为文件控制信息模板的记录数据长度（不包括Tag、Length），84 0E 31 50 41 59 2E 53 59 2E 44 44 46 30 31 A5 03 88 01 01为21字节的记录数据。‘84’为DF名称的记录标识，‘0E’为DF名称的记录数据长度（不包括Tag、Length），31 50 41 59 2E 53 59 53 2E 44 44 46 30 31为14字节的记录数

据，即MF的名称1PAY.SYS.DDF01。‘A5’为文件控制信息专用模板的记录标识，‘03’为文件控制信息专用模板的记录数据长度（不包括Tag、Length），88 01 01为3字节的记录数据。‘88’为DIR短文件标识符的记录标识，‘01’为DIR短文件标识符的记录数据长度（不包括Tag、Length），‘01’为1字节的记录数据，即目录基本文件（DIR）的短文件标识符。

2。DIR为变长记录文件，读目录基本文件（DIR）的第一条记录，则命令为：

00 B2 01 0C 00

由卡片返回的响应数据为：6C 13

再发送读记录命令: 00 B2 01 0C 13

由卡片返回的响应数据为：

61 11 4F 09 A0 00 00 00 03 86 98 07 01 50 04 50 42 4F 43 9000

说明：返回的信息为嵌套的TLV格式的变长记录。‘4F’为银行应用目录文件ADF名称的记录标识，‘09’为银行应用目录文件ADF名称的记录数据长度（不包括Tag、Length），‘ A0 00 00 00 03 86 98 07 01’为9字节的记录数据，即银行应用目录文件ADF的名称。

3。建立银行应用目录文件ADF时指定ADF下发卡方专用数据文件的短文件标识符为95，ADF的名称为 ‘A0 00 00 00 03 86 98 07 01’，对ADF进行选择，则命令为：

00 A4 04 00 09 A0 00 00 00 03 86 98 07 01

由卡片返回的响应数据为：

6F 2E 84 09 A0 00 00 00 03 86 98 07 01 A5 21 9F 0C 1E 11 11 22 22 33 33 00 06 03 01 00 06 19 98 08 17 00 00 00 30 19 98 08 15 19 98 12 15 55 66 90 00

说明：返回的信息为嵌套的TLV格式的变长记录。‘6F’为文件控制信息模板的记录标识，‘2E’为文件控制信息模板的记录数据长度（不包括Tag、Length），其后为2E(HEX)字节的记录数据。‘84’为DF名称的记录标识，‘09’为DF名称的记录数据长度（不包括Tag、Length），A0 00 00 00 03 86 98 07 01为9字节的记录数据，即ADF的名称。‘A5’为文件控制信息专用数据的记录标识，‘21’为文件控制信息专用数据的记录数据长度（不包括Tag、Length），其后为21(HEX)字节的记录数据．‘9F0C’为发卡方定义的基本数据文件的文件控制信息的记录标识，‘1E’为发卡方定义的文件控制信息专用数据的记录数据长度（不包括Tag、Length），即标识符为0015的二进制文件的内容（见附录中的应用举例）。‘55 66’为2字节的发卡方自定义FCI数据。

1. 在任何目录下选择主文件MF

CLA	INS	P1	P2	Lc	DATA
00	A4	00	00	02	3F 00

MF将成为当前目录，且当前目录安全状态寄存器的值自动等于MF的安全状态寄存器的值。

当然，也可用SELECT命令对文件‘1PAY.SYS.DDF01’直接选择。

2. 按文件标识符选择当前目录下的文件或下级子目录

控制性文档 振奇智能

CLA	INS	P1	P2	Lc	DATA
00	A4	00	00	02	文件标识符

若选择的文件为子目录时，该目录成为当前目录，且当前目录安全状态寄存器的值变为0。
若选择的文件为EF时，该文件成为当前文件。

3. 通过目录名称选择DF

CLA	INS	P1	P2	Lc	DATA
00	A4	04	00	XX	DF文件名

Lc定义了DF文件名的长度。
当前目录安全状态寄存器的值变为0。

控制性文档
振奇智能

7. 读二进制文件(READ BINARY)

1). 定义和范围

READ BINARY命令用于读取二进制文件的内容（或部分内容）。

控制性文档
握奇智能

2). 命令报文

READ BINARY命令报文编码如下:

代码	值
CLA	00/04
INS	B0
P1	XX
P2	XX
Lc	不存在；（CLA=04时除外）
Data	不存在；（CLA=04时，应包括MAC）
Le	XX

若P1的高三位为100，则低5位为短的文件标识符，P2为读的偏移量。

若P1的最高位不为1，则P1 P2为欲读文件的偏移量，所读的文件为当前文件。

若CLA = 00时,Le表示要读取的字节数，若T = 0且Le为00，则送回警告状态6Cxx请求将Le置为xx并重发该命令。

3). 命令报文数据域

一般情况下，命令报文数据域不存在。当使用安全报文时，命令报文数据域中应包含MAC。

4). 响应报文数据域

该文件被置成线路保护时，若CLA置为00时响应报文不含MAC，CLA置为04时响应报文包含MAC。

5). 响应报文状态码

IC卡可能回送的错误状态码如下所示:

SW1 SW2	意　义
90 00	命令成功执行
67 00	错误的长度
69 81	不是二进制文件
69 82	读的条件不满足
6A 81	不支持此功能（无MF或MF已锁定）
6A 82	未找到文件
6B 00	参数错误（偏移地址超出了EF）

控制性文档 指令智能

[注] 若文件校验不正确，卡将送出所读的数据，并给出警告状态SW1 SW2=6281。若下次重写该文件，卡将重新计算校验。读一个未曾写过数据的二进制文件也将返回‘6281’。

[例1]: 文件标识符为0005的二进制文件，文件主体空间的大小为8个字节，建立时不采用线路保护。

读出自偏移量01开始到文件结束的所有数据，不进行线路保护，则命令为:

00 B0 85 01 00

由卡片返回的响应数据为:

11 22 33 44 55 66 77 9000

[例2]: 文件标识符为0001的二进制文件，文件主体空间的大小为8个字节，建立时采用线路保护。

读出自偏移量00开始到文件结束的所有数据，使用线路保护密钥进行线路保护，则命令为:

04 B0 00 00 04 82 26 99 9B

说明: 由于P1的最高位不为1，则欲写文件的偏移量为00 00，所读的文件为当前文件，82 26 99 9B为使用线路保护密钥生成的4字节MAC码。

由卡片返回的响应数据为:

01 02 03 04 05 FF FF FF 38 F4 EA 15 9000

[例3]: 文件标识符为0005的二进制文件，文件主体空间的大小为8个字节，建立时采用线路加密保护。

读出自偏移量02开始6字节数据，使用线路保护密钥进行线路加密保护，1C BD 1F 23 F5 4F 8C 9A为06 80 00 00 00 00 00 00的加密数据,则命令为:

04 B0 85 02 0C 1C BD 1F 23 F5 4F 8C 9A DC 8B 2D 0F

由卡片返回的响应数据为:

6E 68 85 9B 17 04 7E D9 8A 75 BA 0B 9000

说明：6E 68 85 9B 17 04 7E D9为使用线路保护密钥对数据66 77 88 FF FF FF加密后的结果，8A 75 BA 0B为使用线路保护密钥生成的4字节MAC码。

[注]: 此处使用到的线路保护密钥为线路保护密钥.

控制性文档
握奇智能

8. 读记录文件(READ RECORD)

1). 定义和范围

READ RECORD命令用于读取定长记录文件、循环文件、钱包文件和变长记录文件的内容。IC卡的响应由回送记录组成。

控制性文档
握奇智能

2). 命令报文

READ RECORD命令报文编码如下：

代码	值
CLA	00/04
INS	B2
P1	见表1
P2	见表2
Lc	不存在（CLA=04时除外）
Data	不存在（CLA=04时除外）
Le	表示要读取的字节数

表1：参数P1的含义：

类型	P1的含义
定长记录文件	记录号，若该文件有N条记录，则记录号可以是1-N。
变长记录文件	记录号，若该文件有N条记录，则记录号可以是1-N。 （参数P2含义如下） 记录标识，如按记录标识来读，则P2的低3位必须为‘000’。
循环文件	记录号，最新写入的记录号为01，上1条记录的记录号为02，依次类推...
钱包文件	记录号，最新写入的记录号为01，上1条记录的记录号为02，依次类推...

表2：参数P2的含义

b8	b7	b6	b5	b4	b3	b2	b1	P2的含义
X	X	X	X	X	1	0	0	b4-b8为短文件标识符
0	0	0	0	0	1	0	0	当前文件

控制性文档
握奇智能

3). 命令报文数据域

当无安全报文使用时，命令报文数据域不存在。使用安全报文时，命令报文的数据域中应包含MAC。

4). 响应报文数据域

所有执行成功的READ RECORD命令的响应报文数据域由读取的记录组成。

若该记录文件为线路保护文件且CLA为04则回送的数据还包括4字节的MAC。

5). 响应报文状态码

IC卡可能回送的错误状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
67 00	错误的长度
69 81	命令与文件结构不相容
69 82	读的条件不满足
6A 81	不支持此功能（无MF或MF已锁定）
6A 82	未找到文件
6A 83	未找到记录

若CLA = 04,Le被忽略,并返回整条记录内容,若CLA=00,当Le不等于该记录的实际长度,返回6Cxx请求将Le置为xx重发该命令.

[例1]: 文件标识符为0001的定长记录文件，它有3条记录，每条记录长度为12个字节。

读出定长记录文件中记录号为02的记录，不进行线路保护，则命令为:

00 B2 02 0C 00返回状态6C 0C

重发该命令00 B2 02 0C 0C ,由卡片返回的响应数据为:

01 02 03 04 05 06 07 08 09 0A 0B 0C 9000

说明: 01 02 03 04 05 06 07 08 09 0A 0B 0C为读出的记录号为02的记录的内容。

[例2]: 文件标识符为0003的循环文件，它有3条记录，每条记录长度为12个字节。

读出循环文件中记录号为01的记录，即最新写入的记录，不进行线路保护，则命令为：

00 B2 01 1C 00

卡片返回状态6C 0C,重发该命令00 B2 01 1C 0C

由卡片返回的响应数据为：

11 22 33 44 55 66 77 88 99 AA BB CC 9000

说明：11 22 33 44 55 66 77 88 99 AA BB CC为读出的记录号为01的记录的内容。

[例3]：文件标识符为0007的变长记录文件。

1。按记录标识来读，读出变长记录文件中记录标识为AA的记录，不进行线路保护，则命令为：

00 B2 AA 38 00

说明：由于按记录标识来读，则P2的低3位必须为‘000’。

卡片返回状态6C 03,重发该命令00 B2 AA 38 03

由卡片返回的响应数据为：

AA 01 11 9000

说明：读出的是TLV格式的记录，AA为记录标识，01表示记录数据的长度，11为1个字节的记录数据。

2。按记录号来读，读出变长记录文件中的第1条记录，不进行线路保护，则命令为：

00 B2 01 3C 00

说明：由于按记录号来读，则P2的低3位必须为‘100’。

卡片返回状态6C 03,重发该命令00 B2 01 3C 03

由卡片返回的响应数据为：

AA 01 11 9000

说明：读出的是TLV格式的记录，AA为记录标识，01表示记录数据的长度，11为1个字节的记录数据。

[例4]：文件标识符为0004的钱包文件，它有2条记录，每条记录长度为4个字节。

1. 向钱包中存入1元钱，则命令为：

80 32 00 24 04 00 00 00 01

2. 读出钱包文件中记录号为01的记录，即最新写入的记录，不进行线路保护，则命令为：

00 B2 01 24 00

卡片返回状态6C 04,重发该命令00 B2 01 24 04

由卡片返回的响应数据为：

00 00 00 01 9000

说明：00 00 00 01为钱包的新余额。

[注]：READ RECORD命令使用线路保护密钥进行线路保护。

控制性文档
报告智能

9. 取响应数据GET RESPONSE(仅用于T=0协议)

1). 命令报文

GET RESPONSE命令报文编码如下:

代码	值
CLA	00
INS	C0
P1	00
P2	00
Lc	不存在
Data	不存在
Le	响应的期望数据最大长度

控制性文档
握奇智能

2). 命令报文数据域

命令报文数据域不存在。

3). 响应报文数据域

响应报文数据域的长度由Le的值决定。

4). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
67	00	长度错误（Le大于卡中响应数据长度）
6F	00	卡中无数据可返回

[注]: Le<xx，则其余数据将自动丢失，因此应一次取回xx字节数据。

[例]: 文件标识符为0001的钱包文件，它有2条记录，每条记录长度为4个字节。

1. 向钱包中存入1元钱，则命令为:

   80 32 00 0C 04 00 00 00 01

由卡片返回的响应数据为：

6108

说明：6108表示有8个数据等待取出。

2. 取响应数据，则命令为：

00 C0 00 00 08

由卡片返回的响应数据为：

00 00 00 02 00 00 00 01 9000

说明：00 00 00 02为4字节钱包中的新余额，00 00 00 01为4字节本次扣款金额。

限制性文档
握奇智能

10. 写二进制文件(UPDATE BINARY)

1). 定义和范围

UPDATE BINARY命令用于写二进制文件、FAC秘密钥文件、FAC公开钥文件。

控制性文档
握奇智能

2). 命令报文

UPDATE BINARY命令报文编码如下：

代码	值
CLA	00/04
INS	D6/D0
P1	XX
P2	XX
Lc	XX
Data	写入文件的数据
Le	不存在

若P1的高三位为100，则低5位为短的二进制文件标识符，P2为欲写文件的偏移量。

若P1的最高位不为1，则P1 P2为欲写文件的偏移量，所写的文件为当前文件。

Lc表示要写入的字节数。

1. 若为线路保护，Lc为写入数据的长度+4字节MAC。

2. 若为加密线路保护，Lc为加密后数据的长度+4字节MAC。

3). 命令报文数据域

报文数据包括要写入的新数据。

若为线路保护文件数据域应包含4字节MAC码

若为线路加密保护文件数据域应包含加密后的数据及4字节MAC码

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC可能回送的错误如下所示:

SW1 SW2	意　义
90 00	命令成功执行
67 00	长度错误(Lc域为空)
69 81	不是二进制或FAC密钥文件不可写
69 82	写的条件不满足
69 87	无安全报文
6A 81	不支持此功能（无MF或MF已锁定）
6A 82	未找到文件
6B 00	参数错误（偏移地址超出了EF）

深圳市文档
指令智能

[例1]: 文件标识符为0001的二进制文件，文件主体空间的大小为8个字节，建立时不采用线路保护。

1. 选择二进制文件，则命令为:

   00 A4 00 00 02 00 01
2. 写二进制文件，不进行线路保护，则命令为:

   00 D6 00 00 02 01 02

说明: 由于P1的最高位不为1，则欲写文件的偏移量为00 00，所写的文件为当前文件。

[例2]: 文件标识符为0005的二进制文件，文件主体空间的大小为8个字节，建立时采用线路保护。

写二进制文件，必须使用线路保护密钥进行线路保护，则命令为:

04 D6 85 01 06 11 22 16 0A C8 C5

说明: 由于P1的最3位为100，则低5位表示短文件标识符05，欲写文件的偏移量P2为01，16 0A C8 C5为使用线路保护密钥生成的4字节MAC码。

[例3]: 文件标识符为0005的二进制文件，文件主体空间的大小为8个字节，建立时采用线路加密保护。

写二进制文件，必须使用线路保护密钥进行线路加密保护，则命令为:

04 D6 85 00 0C 19 47 93 07 DF 79 1D 7F 24 1E D0 03

说明: 19 47 93 07 DF 79 1D 7F为使用线路保护密钥对数据01 02 03 04 05 06 07加密后的结果，24 1E D0 03为使用线路保护密钥生成的4字节MAC码。

11. 写记录文件UPDATE RECORD

1). 定义和范围

UPDATE RECORD命令用于写定长或变长记录文件。

控制性文档
振奇智能

2). 命令报文

CASE1：对于定长记录文件UPDATE RECORD的命令报文编码如下：

代码	值
CLA	00/04
INS	DC/D2
P1	记录号
P2	见表1
Lc	XX
Data	写入的数据
Le	不存在

表1：参数P2的含义

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X	1	0	0	b4-b8为短文件标识符
0	0	0	0	0	1	0	0	当前文件

P1为记录号，若该文件有N条记录，则记录号可以是1-N。

Lc表示要写入的字节数。

1. 若为线路保护，Lc为写入数据的长度+4字节MAC。

2. 若为加密线路保护，Lc为加密后数据的长度+4字节MAC。

[例1]：文件标识符为0002的定长记录文件，它有3条记录，每条记录长度为12个字节，建立时不采用线路保护。

写定长记录文件，不进行线路保护，则命令为：

00 DC 01 14 0C 01 02 03 04 05 06 07 08 09 0A 0B 0C

说明：01 02 03 04 05 06 07 08 09 0A 0B 0C为写入的数据。

[例2]：文件标识符为0001的定长记录文件，它有3条记录，每条记录长度为12个字节，且建立

时采用了线路保护。

写定长记录文件，必须使用线路保护密钥进行线路保护，则命令为：

04 DC 01 0C 10 01 02 03 04 05 06 07 08 09 0A 0B 0C 15 BD 23 3C

说明：01 02 03 04 05 06 07 08 0A 0B 0C为写入的数据，15 BD 23 3C为使用线路保护密钥生成的4字节MAC。

[例3]：文件标识符为0001的定长记录文件，它有3条记录，每条记录长度为12个字节，且建立时采用了加密线路保护。

写定长记录文件，必须使用线路保护密钥进行线路加密保护，则命令为：

04 DC 01 0C 14 A5 DF E4 94 0B 63 DC 35 47 1E D8 A8 CD 09 88 43 C9 52 13 A6

说明：A5 DF E4 94 0B 63 DC 35 47 1E D8 A8 CD 09 88 43为使用线路保护密钥对数据01 02 03 04 05 06 07 08 09 0A 0B 0C加密后的结果，C9 52 13 A6为使用线路保护密钥生成的4字节MAC。

CASE2：对于变长记录文件UPDATE RECORD的命令报文编码如下：

代码	值
CLA	00/04
INS	DC/D2
P1	00：建立新记录时P1缺省为00，记录标识在DATA中给出 XX：修改已存在的记录时P1为原记录标识，新记录标识在DATA中给出（修改记录时，P2的低3位必须置为000）
P2	见表1
Lc	XX
Data	写入的数据
Le	不存在

表1：参数P2的含义

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X				b4-b8为短文件标识符
0	0	0	0	0				当前文件
					0	1	0	增加新记录
					0	0	0	修改原记录（记录标识可与原记录相同）

[例]：文件标识符为0001的变长记录文件，建立时不采用线路保护。

1. 在变长记录文件中建立1条记录标识为AA的新记录，不进行线路保护，则命令为：

00 DC 00 0A 04 AA 02 11 22

2. 修改记录标识为AA的记录，同时将记录标识改为CC，不进行线路保护，则命令为:
00 DC AA 08 04 CC 02 33 44

3). 命令报文数据域

命令报文数据域由写入的记录数据组成。

若为线路保护则由写入的记录数据附上4字节MAC组成。

若为线路加密保护则由被加过密的记录数据附上4字节MAC码组成。

控制性文档
握奇智能

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC可能回送的状态如下所示:

SW1 SW2	意　义
90 00	命令成功执行
67 00	长度错误
69 81	当前文件不是定长或变长记录文件
69 82	写的条件不满足
6A 81	不支持此功能（无MF或MF已锁定）
6A 82	未找到文件
6A 83	未找到记录
6A 84	文件无足够空间

[注]: 为保持TimeCOS兼容性，也可用该命令往循环文件中追加一条记录，但必须置P2低三位为010。

[例]: 文件标识符为0003的循环文件，它有2条记录，每条记录长度为12个字节，建立时不采用线路保护。

往循环文件中追加1条记录，不进行线路保护，则命令为:

00 DC 01 1A 0C 11 22 33 44 55 66 77 88 99 AA BB CC

[注]: UPDATE RECORD命令使用线路保护密钥进行线路保护。

12. 解锁口令(UNBLOCK)

1). 定义和范围

UNBLOCK命令用于解锁被锁定的8字节的口令。

控制性文档
握奇智能

2). 命令报文

UNBLOCK命令报文编码如下：

代码	值
CLA	80
INS	2C
P1	00
P2	解锁口令密钥标识号
Lc	10
Data	8字节解锁口令， 8字节新口令
Le	不存在

只有满足该解锁口令使用条件，并且该解锁口令未被锁死时才执行该命令，该命令不改变安全状态寄存器的值。

若解锁口令核对成功，则新口令值取代解锁口令指定的口令密钥的原有口令（不受原口令密钥更改权限的限制），且将口令错误计数器和解锁口令错误计数器恢复成原始值。

若解锁口令失败，则解锁口令可再试次数减1，如果解锁口令锁死，解锁口令无法再被解锁。

建立解锁口令时,其长度必须为8字节.

3). 命令报文数据域

报文数据域由8字节解锁口令， 8字节新口令组成。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能回送的错误状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
69 82	密钥的使用条件不满足
69 83	解锁口令密钥被锁死
6A 83	密钥未找到
6A 86	参数P1 P2不正确

[说明]: 为保持和TimeCOS 1.0兼容提供此命令，但所建的口令密钥长度必须为8字节。

[例]: 密钥标识号为06的口令解锁密钥，使用权F0，更改权EF，错误计数器33，被锁死的口令密钥号为05，8字节的解锁口令为11 22 33 44 55 66 77 88，建立时不采用线路保护。

密钥标识号为05的口令密钥被锁死，对它进行解锁，不进行线路保护，则命令为:

00 2C 00 06 10 11 22 33 44 55 66 77 88 01 02 03 04 05 06 07 08

说明：11 22 33 44 55 66 77 88为8字节解锁口令，01 02 03 04 05 06 07 08为8字节新口令。

[注]: UNBLOCK命令不支持线路保护以及线路加密保护。在金融应用目录下不支持此命令.

深圳市文迪智能

13. 擦除目录文件DF （ERASE DF）

1). 定义和范围

ERASE DF命令用于擦除当前DF下所有文件。

控制性文档
握奇智能

2). 命令报文

ERASE DF命令报文编码如下：

代码	值
CLA	80
INS	0E
P1	00
P2	00
Lc	00
Data	不存在
Le	不存在

3). 命令报文数据域

命令报文数据域不存在。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能回送的错误状态码如下所示：

SW1	SW2	含 义
90	00	命令成功执行
65	81	写EEPROM不成功
69	82	擦除权限不满足

说明： 擦除当前DF下所有文件，擦除DF后即可任意在该DF下建立文件而不受建立权限的

控制，当建立KEY文件后下次再进入DF将受权限控制，因此建议DF的擦除权限应设计为最高，若不允许擦除设为EF即可。擦除DF成功后，DF下所有基本文件EF及下级目录文件DF都将丢失，成为一个空的DF，但DF本身及其DF的各权限及空间大小均不变。

若当前目录为MF，则除MF外卡上所有基本文件EF和目录文件DF均被删除。

控制性文档
握奇智能

14. 设置通讯协议（SET PROTOCOL）

1). 定义和范围

SET PROTOCOL命令用于设置通讯协议。

控制性文档
握奇智能

2). 命令报文

SET PROTOCOL命令报文编码如下：

代码	值
CLA	80
INS	14
P1	00
P2	00
Lc	01
Data	协议参数
Le	不存在

该命令需当前目录为MF且满足擦除权限时才可设置通讯协议。参数最低位为0表示卡片采用T=0通讯协议，1表示卡片采用T=1通讯协议。

参数的缺省值为FF，即使用3.57MHZ晶振,9600bps通讯速率，T=1通讯协议。

[注意]：正常情况下，通讯协议只能从T=1改为T=0。若要求自由改变或希望支持其它通讯速率，订卡时需特殊申明。

3). 命令报文数据域

命令报文数据域为1字节的参数。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
67 00	长度错误
69 82	权限（MF擦除权限）不满足
6A 81	当前目录不是MF或无MF

[例1]　　将通讯协议由T=1改为T=0，则命令为：

80 14 00 00 01 FE

说明：参数为FE(11111110)表示使用3.57MHZ晶振,9600bps通讯速率，T=0通讯协议。

[例2]　　将通迅协议由T=0改为T=1，则命令为:

80 14 00 00 01 FF

说明：参数为FF(11111111)表示使用3.57MHZ晶振,9600bps通讯速率，T=1通讯协议。

控制性文档
指向智能

15. 扣款（DECREASE）

1). 定义和范围

DECREASE命令用于从记录长度小于8字节的钱包中扣款。

控制性文档
握奇智能

2). 命令报文

DECREASE命令编码如下：

代码	值
CLA	80/84
INS	30
P1	00
P2	见表1
Lc	XX
Data	减少的金额
Le	不存在

表1：参数P2的含义

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X	1	0	0	b4-b8为短文件标识符
0	0	0	0	0	1	0	0	当前文件

3). 命令报文数据域

命令报文数据域由减少的金额组成。

若为线路保护则由减少的金额附上4字节MAC组成。

若为线路加密保护则由被加过密的金额附上4字节MAC码组成。

4). 响应报文数据域

响应报文数据域由Lc字节钱包中新的余额和Lc字节本次扣款金额组成。

若为线路保护则由新余额、扣款金额附上4字节MAC组成。

若为线路加密保护则由被加过密的新余额及扣款金额附上4字节MAC码组成。

5). 响应报文状态码

IC卡可能回送的错误状态码如下所示:

SW1 SW2	意　　义
65 81	写EEPROM不成功
67 00	Lc与钱包文件长度不一致
69 81	不是钱包文件
69 85	扣款或存款条件不满足
69 87	无安全报文
6A 82	文件未找到
93 02	线路保护数据错误
94 01	金额不足

深圳性文档
握奇智能

[说明]: 该命令只能对记录长度小于8字节的钱包文件操作。

[例1]: 文件标识符为0003的钱包文件，它有2条记录，每条记录长度为4个字节，建立时不采用线路保护。

从钱包中扣除2元钱，不进行线路保护，则命令为:

80 30 00 1C 04 00 00 00 02

返回的数据为:

00 00 00 07 00 00 00 02 9000

说明: 00 00 00 07为钱包中的新余额，00 00 00 02为本次扣款金额。

[例2]: 文件标识符为0004的钱包文件，它有2条记录，每条记录长度为4个字节，建立时采用线路保护。

从钱包中扣除4元钱，必须使用线路保护密钥进行线路保护，则命令为:

84 30 00 24 08 00 00 00 04 0C C8 CB 57

返回的数据为:

00 00 00 05 00 00 00 04 56 B1 A4 47 9000

说明: 00 00 00 05为钱包中的新余额，00 00 00 04为本次扣款金额， 56 B1 A4 47为使用线路保护密钥生成的4字节MAC码。

[例3]: 文件标识符为0004的钱包文件，它有2条记录，每条记录长度为4个字节，建立时采用线路加密保护。

从钱包中扣除8元钱，必须使用线路保护密钥进行线路加密保护，则命令为:

84 30 00 24 0C A2 CF BA FF 12 60 8D 7C A7 86 43 E4

说明: A2 CF BA FF 12 60 8D 7C为使用线路保护密钥对数据00 00 00 08加密后的结

果，A7 86 43 E4为使用线路保护密钥生成的4字节MAC码。

返回的数据为:

66 96 46 97 46 B3 0D F4 E9 4D D5 59 2E 81 51 27 F9 0E 1F 4F 9000

说明：66 96 46 97 46 B3 0D F4为使用线路保护密钥加密后钱包中的新余额，E9 4D D5 59 2E 81 51 27为使用线路保护密钥加密后本次存款金额，F9 0E 1F 4F使用线路保护密钥生成的4字节MAC码。

[注]: DECREASE命令使用线路保护密钥进行线路保护.

控制性文档
握奇智能

16. 存款（INCREASE）

1). 定义和范围

INCREASE命令用于向记录长度小于8字节的钱包中存款。

控制性文档
握奇智能

2). 命令报文

INCREASE命令的编码如下:

代码	值
CLA	80/84
INS	32
P1	00
P2	见表1
Lc	XX
Data	增加的金额
Le	不存在

表1: 参数P2的含义

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X	1	0	0	b4-b8为短文件标识符
0	0	0	0	0	1	0	0	当前文件

3). 命令报文数据域

命令报文数据域由增加的金额组成。

若为线路保护则由增加的金额附上4字节MAC组成。

若为线路加密保护则由被加过密的金额附上4字节MAC码组成。

4). 响应报文数据域

响应报文数据域由Lc字节钱包中新的余额和Lc字节本次存款金额组成。

若为线路保护则由新余额、存款金额附上4字节MAC组成。

若为线路加密保护则由被加过密的新余额及存款金额附上4字节MAC码组成。

5). 响应报文状态码

IC卡可能回送的错误状态码如下所示:

SW1 SW2	意　　义
62 83	文件校验错误
67 00	Lc与钱包文件长度不一致
69 81	不是钱包文件
69 85	扣款或存款条件不满足
6A 82	文件未找到
93 02	线路保护数据错误
94 01	金额溢出或本次金额为0

深圳性文档 握奇智能

[说明]: 该命令只能对记录长度小于8字节的钱包文件操作。

[例1]: 文件标识符为0004的钱包文件，它有2条记录，每条记录长度为4个字节，建立时不采用线路保护。

向钱包中存入1元钱，不进行线路保护，则命令为:

80 32 00 24 04 00 00 00 01

返回的数据为:

00 00 00 02 00 00 00 01 9000

说明：00 00 00 02为钱包中的新余额，00 00 00 01为本次存款金额。

[例2]: 文件标识符为0004的钱包文件，它有2条记录，每条记录长度为4个字节，建立时采用线路保护。

向钱包中存入3元钱，必须使用线路保护密钥进行线路保护，则命令为:

84 32 00 24 08 00 00 00 03 FC 57 A4 AB

返回的数据为:

00 00 00 04 00 00 00 03 BF 99 5D C5 9000

说明：00 00 00 04为钱包中的新余额，00 00 00 03为本次存款金额，BF 99 5D C5为使用线路保护密钥生成的4字节MAC码。

[例3]: 文件标识符为0004的钱包文件，它有2条记录，每条记录长度为4个字节，建立时采用线路加密保护。

向钱包中存入5元钱，必须使用线路保护密钥进行线路加密保护，则命令为:

84 32 00 24 0C 27 18 C8 F3 FA 4D 4D 38 EB B5 B3 0C

说明：27 18 C8 F3 FA 4D 4D 38为使用线路保护密钥对数据00 00 00 05加密后的结果，EB B5 B3 0C为使用线路保护密钥生成的4字节MAC码。

返回的数据为：

F0 13 DE E3 B1 A7 8B 1C CC 46 93 CC 2B 47 B9 B7 D2 19 35 38 9000

说明：F0 13 DE E3 B1 A7 8B 1C为使用线路保护密钥加密后钱包中的新余额，CC 46 93 CC 2B 47 B9 B7为使用线路保护密钥加密后本次存款金额，D2 19 35 38使用线路保护密钥生成的4字节MAC码。

[注]: INCREASE命令使用线路保护密钥进行线路保护.

控制性文档
握奇智能

17. 数字签名（DIGITAL SIGNATURES）

1). 定义和范围

DIGITAL SIGNATURES命令用秘密钥对数据进行签字。

控制性文档
握奇智能

2). 命令报文

DIGITAL SIGNATURES命令的编码如下:

代码	值
CLA	80
INS	C2
P1 P2	秘密钥标识符
Lc	需进行签字的数据长度
Data	需要签字的数据
Le	不存在

在满足该密钥的使用条件时才能执行此命令。

3). 命令报文数据域

命令报文数据域由需要签字的数据组成。

4). 响应报文数据域

响应报文数据域由签名后的数据组成。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
67 00	错误的长度
69 81	P_1 P_2指定的标识符不是相应的秘密钥文件

69 82	使用条件不满足
6A 82	秘密钥文件未找到

说明：若采用压缩签字，则先将需签字的数据用COMPRESS命令进行压缩(也可在终端上采用其他方法压缩)，把压缩的结果作为需要签字的数据进行签字。

若Lc为00时,表示用卡中压缩好的数据进行签名。

控制性文档 握奇智能

18. 签名认证（SIGNATURES VERIFY）

1). 定义和范围

SIGNATURES VERIFY命令用公开钥对签名数据进行认证。

控制性文档
握奇智能

2). 命令报文

SIGNATURES VERIFY命令的编码如下:

代码	值
CLA	80
INS	C4
P1 P2	公开钥标识符
Lc	签字的长度
Data	本公钥对应的秘密钥所产生的数字签名
Le	不存在

[说明]: 若P1P2=0000时,表示使用卡内临时公钥进行验证。该临时公钥由COMPRESS命令分批送入。COMPRESS命令除对临时公钥进行压缩以便卡中公钥对该临时公钥作认证外,还保存该临时公钥用于对其他签名进行验证以及对数据进行加密。

3). 命令报文数据域

命令报文数据域由本公钥对应的秘密钥所产生的数字签名数据组成。

4). 响应报文数据域

响应报文数据域由认证后的数据组成。

5). 响应报文状态码

IC卡可能回送的错误状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行

67 00	错误的长度
69 81	P_1 P_2指定的标识符不是相应的公开钥文件
69 82	使用条件不满足
6A 82	公开钥文件未找到

控制性文档
握奇智能

19. FAC数据加密（DATA ENCRYPT）

1). 定义和范围

DATA ENCRYPT命令用非对称密码算法的公开钥对数据进行加密。

控制性文档
握奇智能

2). 命令报文

DATA ENCRYPT命令的编码如下:

代码	值
CLA	80
INS	C6
P1 P2	公开钥标识符
Lc	需加密的数据的长度
Data	需加密的数据
Le	不存在

[说明]: 若P1P2=0000时,表示用临时公钥对数据进行加密。

3). 命令报文数据域

命令报文数据域由需加密的数据组成。

4). 响应报文数据域

响应报文数据域由加密后的密文组成。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
67 00	错误的长度
69 81	P_1 P_2指定的标识符不是相应的公开钥文件

69 82	使用条件不满足
6A 82	公开钥文件未找到

控制性文档
握奇智能

20. FAC数据解密（DATA DECRYPT）

1). 定义和范围

DATA DECRYPT命令用非对称密码算法的秘密钥对加密数据进行解密。

控制性文档
握奇智能

2). 命令报文

DATA DECRYPT命令的编码如下:

代码	值
CLA	80
INS	C8
P1 P2	秘密钥标识符
Lc	需解密的密文的长度
Data	需解密的密文
Le	不存在

在满足该密钥的使用条件时才能执行此命令。

3). 命令报文数据域

命令报文数据域由需解密的密文组成。

4). 响应报文数据域

响应报文数据域由解密后的明文组成。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
67 00	错误的长度
69 81	P_1 P_2指定的标识符不是相应的秘密钥文件

69 82	使用条件不满足
6A 82	秘密钥文件未找到

控制性文档
握奇智能

21. 数据压缩（DATA COMPRESS）

1). 定义与范围

该命令用安全散列算法SHA将数据压缩为20字节，用于FAC签名或验证时使用。

控制性文档
握奇智能

2). 命令报文

DATA COMPRESS命令的编码如下：

代码	值
CLA	80
INS	CC
P1 P2	见以下说明
Lc	数据长度
Data	待压缩的数据
Le	20h

[说明]: 若数据总长度小于138字节，直接对该数据进行压缩；否则以64字节为一块重复执行此指令进行分块压缩，压缩结果由最后一块数据产生。

参数P1的最高位为0时,表示首块数据,否则表示后续块数据;次高位为0时表示输入数据保留在卡内以便其他命令需要时使用,否则输入数据不保留。P1的低六位及P2表示需压缩数据的总长度，当所有表示长度的位均为1时,表示中间块数据,否则,表示最后一块数据。

当进行分块压缩时，除对最后一块数据压缩，卡片只回送9000，并不返回压缩结果。只有对最后一块数据进行压缩时，卡片才返回压缩结果。

3). 命令报文数据域

命令报文数据域包括待压缩的数据。

4). 响应报文数据域

响应报文数据域可能不存在或20字节压缩的结果数据。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
67 00	错误的长度
6A 81	不支持此命令（卡片锁死或无MF）

控制性文档 指令集

[例1]: 对长度为64字节的数据进行压缩，压缩结果由DATA产生，则命令为:

80 CC 00 40 40 DATA（64个0）

返回的数据为:

C8 D7 D0 EF 0E ED FA 82 D2 EA 1A A5 92 84 5B 9A 6D 4B 02 B7 9000

说明: C8 D7 D0 EF 0E ED FA 82 D2 EA 1A A5 92 84 5B 9A 6D 4B 02 B7为20字节的压缩结果。

[注]:对总长度小于等于138字节的数据进行压缩，可参考例1。

[例2]: 对长度为160字节的数据进行压缩，压缩结果由DATA3产生，则命令为:

1. 对第一块数据进行压缩

   80 CC 3F FF 40 DATA1（64个0）

   返回的状态为:

   9000

2. 对中间数据块进行压缩

   80 CC BF FF 40 DATA2（64个0）

   返回的状态为:

   9000

3. 对最后一块数据进行压缩

   80 CC 80 A0 20 DATA3（32个0）

   返回的数据和状态为:

   97 97 ED F8 D0 EE D3 6B 1C F9 25 47 81 60 51 C8 AF 4E 45 EE 9000

说明: 97 97 ED F8 D0 EE D3 6B 1C F9 25 47 81 60 51 C8 AF 4E 45 EE为20字节的压缩结果。

[注]:对数据总长度大于138字节的数据进行压缩，可参考例2。

22. 增加或修改密钥（WRITE KEY）

1). 定义与范围

WRITE KEY命令可向卡中装载密钥或更新卡片中已存在的密钥。

控制性文档
握奇智能

2). 命令报文

WRITE KEY命令的编码如下:

代码	值
CLA	80h/84h
INS	D4
P1	01（用于装载新密钥） 密钥类型（用于密钥更新）
P2	密钥标识
Lc	数据长度
Data	（密钥头 + ）密钥数据
Le	不存在

密钥头（即密钥属性，每种属性占用一字节）定义如下:

密钥类型字节定义如下:

密钥名称	类型字节	密钥名称	类型字节
DES加密密钥	30（HEX）	外部认证密钥	39（HEX）
DES解密密钥	31（HEX）	修改透支限额密钥	3C（HEX）
DESMAC密钥	32（HEX）	圈提密钥	3D（HEX）
内部密钥	34（HEX）	消费密钥	3E（HEX）
线路保护密钥	36（HEX）	圈存密钥	3F（HEX）
口令解锁密钥	37（HEX）	口令（PIN）	3A（HEX）
口令重装密钥	38（HEX）	解锁口令	3B（HEX）

密钥的其他属性详见以下列表:

- DES加密、DES解密、DESMAC、内部密钥、消费、圈提、圈存、修改透支限额密钥的密

钥属性定义如下（密钥长度为8/16字节）：

密钥类型	使用权	更改权	密钥版本号	算法标识
30/31/32/34/3C/3D/3E/3F	由用户定义	由用户定义	由用户定义	01

- 外部认证密钥（密钥长度为8/16字节），密钥标识为00的外部认证密钥又称为主控密钥，主控密钥除用于外部认证以获得某种安全状态外，还控制着密钥的装载和更新：

密钥类型	使用权	更改权	后续状态	错误计数器
39	由用户定义	由用户定义	由用户定义	由用户定义

- 口令密钥（2～8字节），用于口令验证以获得某种安全状态。口令密钥不允许使用线路保护模式装载：

密钥类型	使用权	保留	后续状态	错误计数器
3A	由用户定义	EF	由用户定义	由用户定义

- 解锁口令密钥（8字节），用于解锁指定的被锁定的8字节口令：

密钥类型	使用权	更改权	指定需解锁的口令标识	错误计数器
3B	由用户定义	由用户定义	由用户定义	由用户定义

- 线路保护密钥、口令解锁密钥、重装口令密钥（8/16字节），线路保护密钥用于保护数据的安全传输，口令解锁密钥用于解锁当前应用下被锁定的第一个口令密钥，重装口令密钥用于重装当前应用下被锁定的第一个口令密钥。

密钥类型	使用权	更改权	保留	错误计数器
36/37/38	由用户定义	由用户定义	FF	由用户定义

说明：　密钥标识不可为FF.

内部密钥是用于产生内部临时密钥的密钥。

密钥具有线路保护属性，当使用线路加密方式时，置密钥类型字节次高位为1；当使用线路加密认证方式时，置密钥类型字节最高位和次高位为1；密钥不允许采用认证方式的线路保护属性。

控制性文档 报审稿

具有线路保护属性的密钥（主控密钥除外）必须用相应的线路保护模式装载和修改。采用线路保护模式装载和修改时使用的线路保护密钥为当前应用的主控密钥KActl。

应用（MF除外）主控密钥若具有线路保护属性，装载时使用上一级目录下的应用主控密钥做为线路保护密钥；修改时使用当前应用的主控密钥作为线路保护密钥。

MF下的主控密钥在装载时，采用明文方式；修改时，使用相应的线路保护模式，如需使用线路加密或线路加密认证方式时，使用MF下的主控密钥作为线路保护密钥。

在DF（MF下除外）下装载（增加）密钥时，Lc可以等于1，此时DATA域为1字节密钥属性。采用此种方法装载的密钥，其真正的密钥属性和内容为MF下相对应的密钥类型和标识的密钥属性和内容。如果使用此种方式装载密钥，则该密钥在卡内所用物理空间为3字节。

软件生成文档
推荐使用

[注]：在一个应用下只能有一个口令解锁密钥，一个重装口令密钥，一个主控密钥。

如果该目录下某类型密钥只有一个,则其密钥标识原则上应为‘00’,否则,应从‘01’顺序开始。

使用权限：　指该密钥在使用时如核对、认证、运算时所需满足的条件。

例如：　使用权为41表示在使用该密钥时当前目录安全状态寄存器值必须大于等于1且小于等于4。

更改权限：　指用WRITE KEY更改密钥内容的权限,在满足该条件时可使用WRITE KEY更改密钥内容，但不能改变错误计数器的值。

错误计数器：高半字节指出密钥可以连续错误的最多次数，低半字节指出还可以再试的次数。如果连续错误错超过规定的次数，密钥自动被锁死。

例如：　错误计数器的值为33，表示该密钥最多可以连续错误3次，若输错一次则其值变为32，再错一次之后变为31，若下次核对或认证正确则该值变为33。

使用解锁口令时，解锁口令正确后错误次数低半字节被设置成高半字节值，同时口令被修改。解锁口令若错误，解锁口令允许再试次数减一，解锁口令和外部认证密钥锁死后无法被解锁。

后续状态：当口令核对成功或外部认证成功后，置安全状态寄存器值为后续状态的低半字。

解锁KID(指定需解锁的口令标识)：　当解锁口令核对成功后，想要解开的口令密钥的密钥标识，即要解锁哪个口令密钥。

修改密钥说明:

口令密钥不允许使用此命令进行修改。

任何密钥的密钥头（即密钥属性）不允许修改。

修改密钥时，命令报文不包括密钥头（密钥属性）。

具有线路保护属性的密钥在修改时，必须使用相应的线路保护。线路保护使用的密钥为当前应用的主控密钥。

无论密钥是否具有线路保护属性，参数P1所指的密钥类型均未包含线路保护属性，即P1的最高位和次高位均为0。

密钥被锁死不能使用该命令修改密钥。

控制性文档
振奇智能

3). 命令报文数据域

命令报文数据域包括（密钥头和）密钥内容，如使用线路保护模式，则还包括4字节报文鉴别码。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
67 00	密钥长度错误
69 82	增加或修改权限不满足
69 83	密钥被锁死
6A 82	KEY文件未找到
6A 83	密钥未找到
6A 84	KEY文件空间已满
93 02	修改密钥时线路保护错误

23. 建立文件（CREATE FILE）

1). 定义与范围

CREATE FILE命令用于建立文件系统。

控制性文档
握奇智能

2). 命令报文

CREATE FILE命令的编码如下：

代码	值
CLA	80
INS	E0
P1 P2	文件标识（FileID）
Lc	数据长度
Data	文件控制信息（和 DF 名称）
Le	不存在

3). 命令报文数据域

命令报文数据域包括文件控制信息，如果建立的文件为DF，则还可能包括DF的名称。DF的名称长度为2~16字节。各种文件的控制信息列表如下：

- 目录文件DF（包括MF）

文件类型	文件空间	建立权限	擦除权限	保留字	DF名称
38	2字节	1字节	1字节	3字节FF	5~16字节

说明：建立MF时，P1 P2参数固定为3F 00，文件空间为FF FF。保留字和DF名称域为卡片8字节的传输代码，该传输代码在订货时约定，默认值为8字节FF。

目录文件（MF除外）建立后不能被自动选择。

- 基本文件EF（包括密钥文件）

	命令报文数据域					
文件类型	Byte 1	Byte 2~3	Byte 4	Byte 5	Byte 6	Byte 7
二进制文件	‘28’	文件空间	读权限	写权限	‘FF’	见说明
定长记录文件	‘2A’	文件空间	读权限	写权限	‘FF’	见说明
循环文件	‘2E’	文件空间	读权限	写权限	‘FF’	见说明

普通钱包文件	‘2F’	文件空间		读/扣款权限	存款权限	‘FF’	见说明
PBOC ED/EP		‘02’	‘08’	使用权限	TAC密钥标识符	‘FF’	交易明细文件短标识
变长记录文件	‘2C’	文件空间		读权限	写权限	‘FF’	见说明
FAC公钥文件	‘3D’	文件空间		使用权限	修改权限	读权限	‘FF’
FAC私钥文件	‘3E’	文件空间		使用权限	修改权限	读权限	‘FF’
密钥文件	‘3F’	文件空间		DF文件短标识符	增加权限	‘FF’	‘FF’

控制性文档 报告后销毁

说明:

- 基本文件EF（密钥文件、公钥/私钥文件、PBOC ED/EP文件除外）的Byte1字节称为文件类型字节。文件具有线路保护属性，使用文件类型字节的最高2位表示，当使用线路认证方式时，置文件类型字节最高位为1；当使用线路加密认证方式时，置密钥类型字节最高位和次高位为1。具有线路保护属性的文件，在UPDATE时必须使用相应的线路保护模式，READ时按下列规定使用明文方式或相应的线路保护模式。
- 基本文件EF（密钥文件、公钥/私钥文件、PBOC ED/EP文件除外）的保留字的最后一字节定义如下（设该字节的位定义为b8~b1）：

  i）、b8 = 1时表示该文件不支持带线路保护读，即读二进制、读记录命令使用CLA=04H时，卡片返回状态6E00；b8 = 0表示该文件必须使用线路保护读，即读二进制、读记录命令必须使用CLA = 04，CLA不为04时，卡片返回6E00。

  ii）、b7~b5位保留为1。

  iii）、b4~b3为读（对普通钱包文件还包括扣款操作）操作时使用的密钥标识（11表示使用标识00的线路保护密钥、10表示使用标识01的线路保护密钥、01表示使用标识为02的线路保护密钥，00表示使用标识03的线路保护密钥）

  iv）、b2~b1为写操作（对普通钱包文件为存款操作）时使用的密钥标识（具体对应关系参见iii）。
- 对于记录文件（包括定长记录文件、循环文件、钱包文件），文件空间第1字节为记录总个数，第二字节为记录长度，物理空间总数为（个数*（记录长度+1））。
- 公钥和私钥文件如设置成可读时，只能使用明文方式读取该密钥内容。
- FAC公钥和私钥文件的标识高字节不能为 ‘00’ 。
- 对于密钥文件中所谓DF文件短标识符，说明如下：当高三位为000时，为DDF的短文件标识，当高三位为100时，为ADF的短文件标识。
- 对于PBOC ED/EP中所谓TAC密钥标识是指该ED/EP在计算TAC时使用到的密钥类

型为‘34’的密钥的标识；所谓交易明细文件短标识是指该ED/EP在记录交易明细时所用到的文件短标识符。

- 普通钱包文件的记录长度必须小于8字节。
- 所有文件建立后不能够自动被选择。

控制性文档
握奇智能

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能返回的状态码如下：

SW1 SW2	意义
90 00	命令成功执行
67 00	错误的长度
69 82	建立权限不满足
6A 80	记录个数小于2或目录级数超过三级
6A 84	文件无足够空间
6A 86	文件已存在

24. 验证并修改口令（VERIFY&CHANGE PIN）

1). 定义和范围

VERIFY&CHANGE PIN命令用于核对并修改8字节口令。若核对成功，则安全状态寄存器被置为该口令密钥的后续状态，并用新口令取代旧口令，错误计数器被恢复；若核对不成功，则可再试次数减一，且不修改口令值。

控制性文档
握奇智能

2). 命令报文

VERIFY&CHANGE PIN命令报文如下表:

代码	值
CLA	80/84
INS	24
P1	00
P2	口令密钥标识符
Lc	10
Data	8字节旧口令　8字节新口令
Le	不存在

3). 命令报文数据域

命令报文数据域由8字节旧口令和8字节新口令组成。

若为线路保护则由8字节旧口令和8字节新口令附上4字节MAC码组成。

若为线路加密保护则由被加过密的8字节旧口令和8字节新口令附上4字节MAC码组成。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1 SW2	意　　义

90 00	命令成功执行
63Cx	还剩x次可试机会
6A 82	KEY文件未找到
6A 86	参数P1 P2不正确
93 02	安全报文数据项不正确
93 03	应用永久锁定
94 03	密钥未找到

[注]: VERIFY&CHANGE命令使用口令解锁密钥密钥进行线路保护。

控制性文档
指令智能

七. 中国金融IC卡专用命令

控制性文档
握奇智能

1. 卡片锁定（CARD BLOCK）

1). 定义和范围

CARD BLOCK命令使卡中所有应用永久失效。

当CARD BLOCK命令成功地完成后，所有后续的命令都将回送状态码“不支持此功能”（SW1 SW2=‘6A81’），且不执行任何其它操作。

2). 命令报文

CARD BLOCK命令报文编码如下:

代码	值
CLA	84
INS	16
P1	00
P2	00
Lc	04
Data	MAC（由16字节线路保护密钥生成）
Le	不存在

3). 命令报文数据域

命令报文数据域包括报文鉴别代码（MAC）数据元。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
64	00	状态标志未改变
65	81	写EEPROM不成功
69	87	安全报文数据项丢失
69	88	安全报文数据项不正确

控制性文档
握奇智能

2. 应用解锁（APPLICATION UNBLOCK）

1). 定义和范围

APPLICATION UNBLOCK命令用于恢复当前的应用。

当APPLICATION UNBLOCK命令成功地完成后，用APPLICATION BLOCK命令产生的对应用命令响应的限制将被取消。

如果对某应用连续三次解锁失败，则IC卡将永久锁定此应用。

控制性文档 握奇智能

2） 命令报文

APPLICATION UNBLOCK命令报文编码如下:

代码	值
CLA	84
INS	18
P1	00
P2	00
Lc	04
Data	MAC（由16字节线路保护密钥生成）
Le	不存在

3). 命令报文数据域

命令报文数据域包括报文鉴别代码（MAC）数据元。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

无论应用是否已经失效，此命令执行成功的状态码是‘9000’。

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
69	82	不满足安全状态
69	83	认证方式锁定
69	88	安全报文数据项不正确
93	03	应用永久锁定

控制性文档
握奇智能

3. 应用锁定（APPLICATION BLOCK）

1). 定义和范围

APPLICATION BLOCK命令使当前选择的应用失效。

当APPLICATION BLOCK命令成功地完成后，用SELECT命令选择已失效的应用，将回送状态码“选择文件无效”（SW1 SW2=‘6A81’）。

控制性文档
握奇智能

2). 命令报文

APPLICATION BLOCK命令报文编码如下:

代码	值
CLA	84
INS	1E
P1	00
P2	00/01
Lc	04
Data	MAC（由线路保护密钥生成）
Le	不存在

P=00: 此命令执行成功后可锁定应用，但该应用可以用APPLICATION UNBLOCK命令解锁，可由SELECT命令选择进入该目录，但对文件操作时返回6A81。

P=01: 此命令执行成功后将永久锁定应用，IC卡将设置一个内部标志以表明不允许执行APPLICATION UNBLOCK命令，可由SELECT命令选择进入该目录，但对文件操作时返回6A81。

3). 命令报文数据域

命令报文数据域包括报文鉴别代码（MAC）数据元。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

无论应用是否已经失效，此命令执行成功的状态码是‘9000’。

IC卡可能回送的错误状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
65	81	写EEPROM不成功
69	82	不满足安全状态
6A	86	参数P1 P2不正确
69	88	安全报文数据项不正确

注册生文档 指南智能

4. 口令密钥解锁（PIN UNBLOCK）

1). 定义与范围

PIN UNBLOCK命令发卡方提供了解锁口令密钥的功能。

当PIN UNBLOCK命令成功完成后，卡片将重置个人密码错误计数器的值。

命令中口令密钥的传递采用加密方式。

控制性文档
握奇智能

2). 命令报文

PIN UNBLOCK命令报文编码如下:

代码	值
CLA	84
INS	24
P1	00
P2	01
Lc	0C
Data	加密的口令密钥数据元和报文鉴别码（MAC）数据元
Le	不存在

[注]: 此处的Data为口令解锁密钥对原口令值进行加密和计算MAC.

3). 命令报文数据域

命令报文数据域由口令密钥数据元和其后的报文鉴别代码（MAC）数据元组成。

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1 SW2	意　　义
90 00	命令成功执行
69 82	不满足安全状态
6A 82	KEY文件未找到
6A 86	参数P1 P2不正确
69 88	安全报文数据项不正确
93 03	应用永久锁定
94 03	密钥未找到

保密性文档
握奇智能

[例1]：密钥标识符为00的口令密钥被锁死，对该口令密钥进行解锁，必须使用口令解锁密钥进行线路保护，则命令为：

84 24 00 01 0C F3 97 B1 FD 0C D1 74 7A 8E 0C B9 3B

由卡片返回的响应数据为：

9000

说明：在解锁口令密钥命令报文中并不能指定口令密钥的密钥标识符，系统将自动对密钥文件中标识为00的口令密钥进行解锁。

5. 重装/修改口令密钥（RELOAD/CHANGE PIN）

1). 定义与范围

RELOAD/CHANGE PIN命令用于发卡方重新给持卡人产生一个新的PIN。

RELOAD/CHANGE PIN只能在能访问到重装口令密钥的发卡方终端或拥有原口令时才能够执行。

在成功执行RELOAD/CHANGE PIN命令后，IC卡必须完成以下操作:

1. 密钥错误尝试计数器复位。
2. IC卡的原密钥必须设置为新的值。

2). 命令报文

RELOAD/CHANGE PIN命令报文编码如下:

代码	值
CLA	80
INS	5E
P1	00：RELOAD PIN 01：CHANGE PIN
P2	00
Lc	数据长度
Data	重装的PIN和报文鉴别码MAC（RELOAD PIN） 旧口令 ‖ FF ‖ 新口令（CHANGE PIN）
Le	不存在

3). 命令报文数据域

重装口令（RELOAD PIN）时包括PIN值和报文鉴别码MAC，此处的MAC是由重装口令密钥前后8字节异或后的结果口令PIN值进行MAC计算的结果，且MAC计算的初始值为8个00。

修改口令（CHANGE PIN）时包括原口令值和 FF 和新口令值。

控制性文档 握奇智能

4). 响应报文数据域

响应报文数据域不存在。

5). 响应报文状态码

IC卡可能回送的错误状态码如下所示：

SW1	SW2	含义
90	00	命令成功执行
67	00	长度错误
69	82	不满足安全状态
69	83	认证方式锁定
69	85	使用条件不满足
69	88	MAC错误
93	03	应用永久锁定
94	03	密钥未找到

[例1]：密钥文件中有一个密钥标识符为00，长度为6字节的口令密钥，发卡方重新给持卡人产生一个新的口令密钥，则命令为：

80 5E 00 00 0A 22 33 44 55 66 77 1C E6 AA 60

说明：22 33 44 55 66 77为重装的6字节新口令，1C E6 AA 60为4字节的MAC码，但应特别注意的是此处的MAC是由重装口令密钥前后8字节相异或后对6字节新口令值计算的MAC。

由卡片返回的状态码为：

9000

[例2]：密钥文件中有一个密钥标识符为00，长度为2字节的口令密钥，修改该口令密钥进行解锁，则命令为：

84 5E 01 00 05 00 00 FF 31 32

说明：00 00为旧的口令密钥，31 32为新的口令密钥。

由卡片返回的响应数据为：

9000

说明：在重装口令密钥命令报文中并不能指定口令密钥的密钥标识符，系统将自动对密钥文件中标识为00的口令密钥进行重装。

证制性文档
握奇智能

6. 圈存（CREDIT FOR LOAD）

1). 定义与范围

通过圈存交易，持卡人可将其在银行相应帐户上的资金划入电子存折或电子钱包中。这种交易必须在金融终端上联机进行并要求验证口令（无论电子存折还是电子钱包应用）。

控制性文档
振奇智能

2). 圈存初始化命令报文

在进行圈存交易之前，必须进行圈存初始化，圈存初始化（INITIALIZE FOR LOAD）命令报文如下:

代码	值
CLA	80
INS	50
P1	00
P2	01：用于电子存折; 02：用于电子钱包。
Lc	0B
Data	1字节密钥标识符　4字节交易金额　6字节终端机编号
Le	10

3). 圈存初始化命令报文数据域

圈存初始化命令报文数据域包括以下数据元:

说明	长度（字节）
密钥标识符（圈存密钥）	1
交易金额	4
终端机编号	6

4). 圈存初始化响应报文数据域

此命令执行成功的响应报文数据域如下表:

说明	长度（字节）
电子存折或电子钱包旧余额	4
电子存折或电子钱包联机交易序号	2
密钥版本号（DATA中第一字节指定的圈存密钥的密钥版本号）	1
算法标识（DATA中第一字节指定的圈存密钥）	1
伪随机数（IC卡）	4
MAC1	4

控制性文档 握奇智能

过程密钥由DATA中第一字节即密钥标识符指定的圈存密钥对（4字节随机数+2字节电子存折或电子钱包联机交易序号+80 00）数据加密生成。

MAC1由卡中过程密钥对（4字节电子存折或电子钱包旧余额+4字节交易金额+1字节交易类型标识+6字节终端机编号）数据加密生成。

交易类型标识:

值	含义
01	电子存折圈存
02	电子钱包圈存
03	圈提
04	电子存折取款
05	电子存折消费
06	电子钱包消费
07	电子存折修改透支限额

5). 圈存初始化响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
67	00	长度错误
6A	81	功能不支持（无MF或卡片已锁死）
6A	86	参数P1 P2错误
94	03	密钥未找到

6). 圈存命令报文

CREDIT FOR LOAD命令报文编码如下:

代码	值
CLA	80
INS	52
P1	00
P2	00
Lc	0B
Data	交易日期 交易时间 MAC2
Le	04

控制性文档
握奇智能

7). 圈存命令报文数据域

圈存命令报文数据域包括以下数据元:

说明	长度（字节）
交易日期（主机）	4
交易时间（主机）	3
MAC2	4

MAC2由卡中过程密钥对（4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节主机交易日期+3字节主机交易时间）数据加密生成。

8). 圈存命令响应报文数据域

此命令执行成功的响应报文数据域如下表:

说明	长度（字节）
交易验证码TAC	4

TAC用内部密钥DTK（专门用于生成TAC的密钥，见附录）左右8位字节异或运算的结果对（4字节电子存折或电子钱包新余额+2字节电子存折或电子钱包联机交易序号（加1前）+4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节主机交易日期+3字节主机交易时间）数据加密生成。

9). 圈存命令响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
67	00	长度错误
69	01	命令不接受（无效状态）
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持（无MF或卡片已锁死）
93	02	MAC无效

[注]: 完成圈存交易后，IC卡把交易金额加在电子存折或电子钱包的余额上，将电子存折或电子钱包联机交易序号加1，并用下表的数据组成一个记录，保存在电子存折或电子钱包所指定的记录长度为23个字节的交易明细文件中。

说明	长度（字节）
电子存折或电子钱包联机交易序号	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
主机交易日期	4
主机交易时间	3

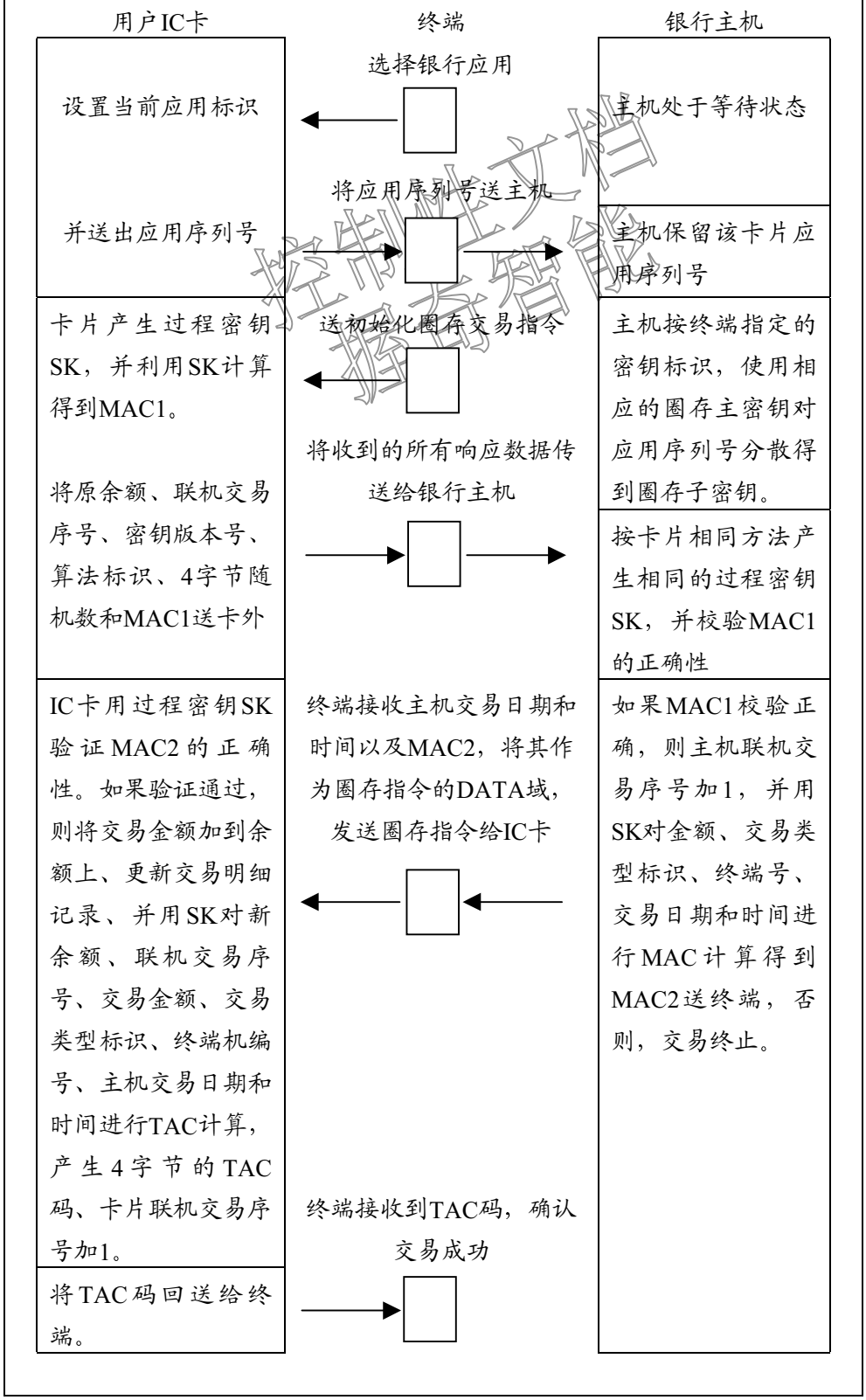
[注]: 在银行的应用目录下，圈存交易过程中所有MAC及TAC的生成过程见第八章中《MAC的计算》，唯一的区别是将8个字节的 ‘00 00 00 00 00 00 00 00’作为初始值。TAC的生成方法与MAC完全相同。

10). 圈存交易流程

在进行圈存交易时，先选择银行应用，然后在银行应用下进行操作，下面就整个过程列表如下:

恒指性文档 指尚智能

圈存交易流程表



控制性文档
指导智能

7. 消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）

1). 定义与范围

消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令用于消费/取现交易。

消费交易允许持卡人使用电子存折或电子钱包的余额进行购物或获取服务。此交易可以在销售点终端（POS）上脱机进行。使用电子存折进行的消费交易必须验证口令，使用电子钱包则不需要。

取现交易允许持卡人从电子存折中提取现金。此交易必须在金融终端上进行，但可以脱机处理。只有电子存折应用支持此交易，且必须验证口令。

控制性文档
指令智能

2). 消费/取现初始化命令报文

在进行消费/取现交易之前，必须初始化消费/取现交易。初始化消费/取现交易（INITIALIZE FOR PURCHARSE/CASH WITHDRAW）命令报文如下:

代码	值
CLA	80
INS	50
P1	01：消费初始化 02：取现初始化
P2	01：用于电子存折; 02：用于电子钱包（取现交易不支持）
Lc	0B
Data	1字节密钥标识符　4字节交易金额　6字节终端机编号
Le	0F

3). 消费/取现初始化命令报文数据域

消费/取现初始化命令报文数据域包括以下数据元:

说明	长度（字节）
密钥标识符（消费密钥）	1
交易金额	4
终端机编号	6

4). 消费/取现初始化响应报文数据域

此命令执行成功的响应报文数据域如下表:

说明	长度（字节）
电子存折或电子钱包旧余额	4
电子存折或电子钱包脱机交易序号	2
透支限额	3
密钥版本号（DATA中第一字节指定的消费密钥的版本号）	1
算法标识（DATA中第一字节指定的消费密钥的算法标识）	1
伪随机数（IC卡）	4

控制性文档 指向智能

5). 消费/取现初始化响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持（卡片或应用已锁死）
6A	82	文件未找到
94	01	金额不足

6). 消费/取现命令报文

DEBIT FOR PURCHASE命令报文编码如下:

代码	值
CLA	80
INS	54
P1	01
P2	00
Lc	0F
Data	见下表
Le	08

7). 消费/取现命令报文数据域

消费/取现命令报文数据域包括以下数据元:

说明	长度（字节）
终端交易序号	4
交易日期（终端）	4
交易时间（终端）	3
MAC1	4

控制性文档 振奇智能

过程密钥由与消费初始化相同的消费密钥对（4字节随机数+2字节电子存折或电子钱包脱机交易序号+终端交易序号的最右两个字节）数据加密生成。

MAC1由卡中过程密钥对（4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节终端交易日期+3字节终端交易时间）数据加密生成。

8). 消费/取现响应报文数据域

此命令执行成功的响应报文数据域如下表:

说明	长度（字节）
交易验证码TAC	4
MAC2	4

MAC2由卡中过程密钥对（4字节交易金额）数据加密生成。

TAC用内部密钥DTK（专门用于生成TAC的密钥，见附录）左右8位字节异或运算的结果对（4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节终端交易序号+4字节终端交易日期+3字节终端交易时间）数据加密生成。

9). 消费/取现响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
67	00	长度错误
69	01	命令不接受（无效状态）
69	82	不满足安全状态

69	85	使用条件不满足
6A	81	功能不支持（无MF或卡片已锁死）
93	02	MAC无效
94	01	金额不足

[注]：完成消费交易后，IC卡从电子存折或电子钱包余额中扣减消费的金额，将电子存折或电子钱包脱机交易序号加1，并用下表的数据组成一个记录，保存在电子存折所指定记录长度为23个字节的交易明细文件中。（电子钱包不记录交易记录）

说明	长度（字节）
电子存折脱机交易序号	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
终端交易日期	4
终端交易时间	3

10). 消费/取现交易流程

消费交易可以脱机进行，取现交易必须联机进行，且取现交易只能对电子存折进行，现以消费脱机交易为例说明其流程。有关PSAM卡的特性和指令请参见本公司另一文档《PSAM卡手册》，此处用到的MAC1计算及MAC2校验指令属于《PSAM卡手册》的范畴。

江南性文档 指令规范

脱机消费交易流程表

用户IC卡	终端	PSAM卡
设置当前应用标识	选择银行应用	
并送出应用序列号	接收应用序列号并保存	
卡片产生过程密钥SK。 将原余额、脱机交易序号、透支限额、密钥版本号、算法标识、4字节随机数送卡外	送初始化圈存交易指令 将收到的有关数据以及应用序列号作为MAC1计算命令的DATA域，送MAC1计算命令给PSAM卡。	PSAM卡按指定的密钥版本号，使用相应的消费主密钥对应用序列号分散得到消费子密钥。按卡片相同方法产生相同的过程密钥SK，并计算产生MAC1。
IC卡用过程密钥SK验证MAC1的正确性。如果验证通过，则将从余额扣除消费的金额、并用SK对相应数据计算得到4字节的MAC2和4字节的TAC码、卡片脱机交易序号加1。	终端将终端号、交易日期和时间以及MAC1作为圈消费指令的DATA域，发送消费指令给IC卡 终端接收到TAC码，确认交易成功，并将MAC2送PSAM卡校验	将MAC1回送给终端。 如果MAC2校验成功，则终端应记录该笔交易，否则，PSAM卡应用错误计数器减1，当计数器值为0时，PSAM卡将锁死。
将MAC2和TAC码回送给终端。	接收PSAM卡回送的确认	

控制注文档
指向智能

8. 圈提（DEBIT FOR UNLOAD）

1). 定义与范围

通过圈提交易，持卡人可以把电子存折中的部分或全部资金划回到其在银行的相应帐户上。这种交易必须在金融终端上联机进行并要求验证口令。只有电子存折应用支持圈提交易。

控制性文档
握奇智能

2). 圈提初始化命令报文

在进行圈提交易之前，必须进行圈提初始化（INITIALIZE FOR UNLOAD）。

INITIALIZE FOR UNLOAD命令报文编码如下:

代码	值
CLA	80
INS	50
P1	05
P2	01：用于电子存折
Lc	0B
Data	1字节密钥标识符　4字节交易金额　6字节终端机编号
Le	10

3). 圈提初始化命令报文数据域

圈提初始化命令报文数据域包括以下数据元:

说明	长度（字节）
密钥标识符（圈提密钥）	1
交易金额	4
终端机编号	6

4). 圈提初始化响应报文数据域

此命令执行成功的响应报文数据域如下表:

说明	长度
电子存折旧余额	4
电子存折联机交易序号	2
密钥版本号（DATA中第一字节指定的圈提密钥的版本号）	1
算法标识（DATA中第一字节指定的圈提密钥的算法标识）	1
伪随机数（IC卡）	4
MAC1	4

控制性文档 振奇智能

过程密钥由DATA中第一字节即密钥标识符指定的圈提密钥对（4字节随机数+2字节电子存折联机交易序号+8000）数据加密生成。

MAC1由卡中过程密钥对（4字节电子存折旧余额+4字节交易金额+1字节交易类型标识+6字节终端机编号）数据加密生成。

交易类型标识参见圈存交易命令中的有关章节。

5). 圈提初始化响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
67	00	长度错误
69	85	使用条件不满足
6A	81	功能不支持（无MF或卡片已锁死）
6A	86	参数P1 P2错误
94	01	金额不足
94	03	密钥索引不支持

6). 圈提命令报文

CREDIT FOR UNLOAD命令报文编码如下:

代码	值
CLA	80
INS	54
P1	03
P2	00
Lc	0B
Data	见下表
Le	04

控制性文档
握奇智能

7). 圈提命令报文数据域

圈提命令报文数据域包括以下数据元:

说明	长度（字节）
主机交易日期	4
主机交易时间	3
MAC2	4

MAC2由卡中过程密钥对（4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节主机交易日期+3字节主机交易时间）数据加密生成。

8). 圈提响应报文数据域

此命令执行成功的响应报文数据域如下表:

说明	长度（字节）
MAC3	4

MAC3由卡中过程密钥对（4字节电子存折新余额+2字节电子存折联机交易序号(加1前)+4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节主机交易日期+3字节主机交易时间）数据加密生成。

9). 圈提响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
67	00	长度错误
69	01	命令不接受（无效状态）
6A	81	功能不支持（无MF或卡片已锁死）
93	02	MAC无效

控制性文档
指向智能

[注]：完成圈提交易后，IC卡从电子存折余额中扣减交易金额，将电子存折联机交易序号加1，并用下表的数据组成一个记录，保存在电子存折所指定的长度为23字节的交易明细文件中。

说明	长度（字节）
电子存折联机交易序号	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
主机交易日期	4
主机交易时间	3

10). 圈提交易流程

圈提交易只能够针对电子存折。交易流程见下表:

圈提交易流程表

用户IC卡	终端	银行主机
设置当前应用标识	选择银行应用	主机处于等待状态
并送出应用序列号	将应用序列号送主机	主机保留该卡片应用序列号
卡片产生过程密钥SK，并利用SK计算得到MAC1。 将原余额、联机交易序号、密钥版本号、算法标识、4字节随机数和MAC1送卡外	送初始化圈提交易指令 将收到的所有响应数据传送给银行主机	主机按终端指定的密钥标识，使用相应的圈提主密钥对应用序列号分散得到圈提子密钥。 按卡片相同方法产生相同的过程密钥SK，并校验MAC1的正确性
IC卡用过程密钥SK验证MAC2的正确性。如果验证通过，则将从电子存折上扣除交易金额、更新交易明细记录、并用SK对新余额、联机交易序号、交易金额、交易类型标识、终端机编号、主机交易日期和时间进行MAC计算，产生4字节的MAC3、卡片联机交易序号加1。	终端接收主机交易日期和时间以及MAC2，将其作为圈提指令的DATA域，发送圈提指令给IC卡	如果MAC1校验正确，则主机联机交易序号加1，并用SK对金额、交易类型标识、终端号、交易日期和时间进行MAC计算得到MAC2送终端，否则，交易终止。
将MAC3回送给终端。	终端接收到MAC3，送主机验证并保存	主机验证MAC3，并保存以待审计

控制性文档 指向智能

9. 修改透支限额（UPDATE OUVERDRAW LIMIT）

1). 定义与范围

当电子存折中的实际金额不足时，“透支功能”为持卡人提供了一种在发卡方所允许的透支额度内继续进行交易的方便性。修改透支限额交易必须在金融终端上联机进行，且必须验证口令。

控制性文档
握奇智能

2). 修改透支限额初始化命令报文

在修改透支限额命令执行之前，必须进行修改透支限额初始化命令（INITIALIZE FOR UPDATE）。INITIALIZE FOR UPDATE命令报文编码如下:

代码	值
CLA	80
INS	50
P1	04
P2	01：仅用于电子存折
Lc	07
Data	1字节密钥标识符　6字节终端机编号
Le	13

3). 修改透支限额初始化命令报文数据域

修改透支限额初始化命令报文数据域包括以下数据元:

说明	长度（字节）
密钥标识符（修改透支限额密钥）	1
终端机编号	6

4). 修改透支限额初始化响应报文数据域

此命令执行成功的响应报文数据域如下表:

说明	长度（字节）
电子存折旧余额	4
电子存折联机交易序号	2
旧透支限额	3
密钥版本号（DATA中指定的修改透支密钥的版本号）	1
算法标识（DATA中指定的修改透支密钥的算法标识）	1
伪随机数（IC卡）	4
MAC1	4

控制性文档 指令智能

过程密钥由DATA中第一字节指定的修改透支限额密钥对（4字节随机数+2字节电子存折联机交易序号+8000）数据加密生成。

MAC1由卡中过程密钥对（4字节电子存折余额+3字节旧透支限额+1字节交易类型标识+6字节终端机编号）数据加密生成。

5). 修改透支限额初始化响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
67	00	长度错误
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持（无MF或卡片已锁死）
6A	82	文件未找到
6A	86	参数P1 P2错误
94	03	密钥标识不支持

6). 修改透支限额命令报文

UPDATE OVERDRAW LIMIT命令用于修改透支限额交易。编码如下:

代码	值
CLA	80
INS	58
P1	00
P2	00
Lc	0E
Data	见下表
Le	04

控制性文档
振奇智能

7). 修改透支限额命令报文数据域

修改透支限额命令报文数据域包括以下数据元:

说明	长度（字节）
新透支限额	3
发卡方交易日期	4
发卡方交易时间	3
MAC2	4

过程密钥由与修改透支限额初始化相同的修改透支限额密钥对（4字节随机数+2字节电子存折联机交易序号+8000）数据加密生成。

MAC2由卡中过程密钥对（3字节新透支限额+1字节交易类型标识+6字节终端机编号+4字节主机交易日期+3字节主机交易时间）数据加密生成。

8). 修改透支限额响应报文数据域

此命令执行成功的响应报文数据域如下表:

说明	长度（字节）
交易验证码TAC	4

TAC用内部密钥DTK（专门用于生成TAC的密钥，见附录）直接对（4字节电子存折新余额+2字节电子存折联机交易序号(加1前)+3字节电子存折新透支限额+1字节交易类型标识+6字节终端机编号+4字节主机交易日期+3字节主机交易时间）数据加密生成。

9). 修改透支限额响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
67	00	长度错误
69	01	命令不接受（无效状态）
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持（无MF或卡片已锁死）
93	02	MAC无效
94	01	金额不足

[注]: 完成修改透支限额交易后，IC卡将当前电子存折余额置为新的电子存折余额，更新透支限额，使电子存折联机交易序号加1，并用下表的数据组成一个记录，保存在电子存折所指定记录长度为23个字节的交易明细文件中。

说明	长度（字节）
电子存折脱机交易序号	2
新透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
终端交易日期	4

10). 修改透支限额流程

修改透支限额只能对电子存折进行操作，且必须联机执行。

开创性文档 指向智能

修改透支限额交易流程表

用户IC卡	终端	银行主机
设置当前应用标识	选择银行应用	主机处于等待状态
并送出应用序列号	将应用序列号送主机	主机保留该卡片应用序列号
卡片产生过程密钥SK，并利用SK计算得到MAC1。 将原余额、联机交易序号、原透支限额、密钥版本号、算法标识、4字节随机数和MAC1送卡外	初始化修改透支限额指令 将收到的所有响应数据传送给银行主机	主机按终端指定的密钥标识，使用相应的修改透支限额主密钥对应用序列号分散得到修改透支限额子密钥。 按卡片相同方法产生相同的过程密钥SK，并校验MAC1的正确性
IC卡用过程密钥SK验证MAC2的正确性。如果验证通过，则将交易金额加到余额上、更新透支限额、更新交易明细记录、并用SK对新余额、联机交易序号、交易金额、交易类型标识、终端机编号、主机交易日期和时间进行TAC计算，产生4字节的TAC码、卡片联机交易序号加1。	终端接收主机交易日期和时间以及MAC2，作为修改透支限额指令的DATA域，发送该指令给IC卡	如果MAC1校验正确，则主机联机交易序号加1，并用SK对新透支限额、交易类型标识、终端号、交易日期和时间进行MAC计算得到MAC2送终端，否则，交易终止。
将TAC码回送给终端。	终端接收到TAC码，确认交易成功	

招标文档 招商智能

10. 取交易认证码（GET TRANSACTION PROVE）

1). 定义与范围

GET TRANSACTION PROVE命令提供了一种在交易处理过程中拔出并重插卡后卡片的恢复机制。

控制性文档
握奇智能

2). 命令报文

GET TRANSACTION PROVE命令报文编码如下:

代码	值
CLA	80
INS	5A
P1	00
P2	要取MAC或交易验证码所对应的交易类型标识
Lc	02
Data	见表1
Le	04/08

3). 命令报文数据域

表1定义了命令报文的数据域:

说明	长度（字节）
要取MAC或交易验证码所对应的当前的电子存折电子钱包联机或脱机交易序号	2

4). 响应报文数据域

如果命令中指定的交易类型标识和电子存折、电子钱包联机或脱机交易序号对应的报文鉴别代码MAC或交易验证码TAC可用，则响应报文数据域如下表:

说明	长度（字节）
报文鉴别代码MAC（可能不存在）	4
交易验证码TAC	4

5). 响应报文状态码

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持（无MF或卡片已锁死）
6A	82	文件未找到
93	02	MAC无效
94	06	所需MAC不可用

深圳市文档指南智能

6). 防插拔功能

此功能保证卡片在交易处理中的任何情况下，仍能保持数据的完整性。

在终端发给IC卡一个命令以更新电子存折或电子钱包余额时，卡片总会回送一个报文鉴别代码(MAC)或交易验证码(TAC)，以证明更新已经发生。一旦余额更新成功，可以通过GET TRANSCATION PROVE命令获得此MAC或TAC。

如果在命令已执行结束，而终端还未收到响应之前，卡片突然拔出，终端将会处于不知卡片是否更新的不定状态。在这种情况下，终端可以用GET TRANSACTION PROVE命令取回MAC或TAC，如果返回‘9000’则表示卡片更新成功，交易完成。如果不返回‘9000’则表示卡片更新失败，要想完成该交易必须从交易初始化开始重新进行。

11. 读取余额（GET BALANCE）

1). 定义与范围

GET BALANCE命令用于读取电子钱包或电子存折余额，实现查询余额交易。读取电子存折余额需验证口令密钥（PIN）。

控制性文档
握奇智能

2). 命令报文

GET BALANCE命令报文编码如下:

代码	值
CLA	80
INS	5C
P1	00
P2	01：用于电子存折; 02：用于电子钱包
Lc	不存在
Data	不存在
Le	04

3). 命令报文数据域

命令报文数据域不存在。

4). 响应报文数据域

命令执行成功的响应报文数据域如下所示:

说明	长度（字节）
电子存折或电子钱包余额	4

5). 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC卡可能回送的状态码如下所示:

SW1	SW2	含义
90	00	命令成功执行
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持（无MF或卡片已锁死）
6A	82	文件未找到

控制性文档
握奇智能

八. 安全报文传送

控制性文档
指令智能

1. 安全报文传送

卡与外界进行数据传输（卡接收命令，发送应答）时，若以明文方式传输，攻击者通过劫获这些数据，可以分析出卡的结构，掌握卡中的数据。同时，也可以对传输的数据进行篡改。

如何避免这个问题呢？方法就是采用安全报文传送。

安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。安全报文传送有三种情况:

1. 完整性保护

对传输的数据附加4字节MAC码，接收方收到后首先进行校验，只有校验正确的数据才予以接受，这样就防止了对传输数据的篡改。

数据完整性和对发送方的认证通过使用MAC来实现。

2. 机密性保护

对传输的数据进行DES加密，这样传输的就是密文，攻击者即使获得的数据没有意义，分析后也只能得到错误的结果。

数据的机密性通过对数据域的加密来得到保证。

3. 机密性和完整性保护

对传输的数据进行DES加密后再附加4字节MAC码。

[注]: 至于采取哪种方法进行安全报文传送由用户根据实际情况来决定。应该指出，高安全性是以降低速度，增加实现难度来换取的，所以并不是安全性越高越好，而一定要根据具体的要求来确定。

2. 如何实现安全报文传送

二进制文件、定长记录文件、变长记录文件、循环文件、钱包文件都可以采用安全报文传送。如对上述文件进行安全报文传送，只需在建立文件时改变文件类型字节高两位即可:

最高位置1表示数据域附加4字节MAC，次高位置1表示对数据加密。

对于密钥也可以采用安全报文传送。如进行安全报文传送，只需在安装密钥时改变密钥类型字节高两位即可:

最高位置1表示数据域附加4字节MAC，次高位置1表示对数据加密。

例： 建立文件时若需进行线路保护则将文件类型最高位置1，如二进制类型由28变为A8。对密钥若需进行线路加密保护则将密钥类型最高位及次高位均置1，如PIN类型由3A变为FA。

[注]： 在对文件进行读写，或使用密钥（如核对、解锁，认证或更改密钥）时，若需采用安全报文传送，必须置CLA的后半字节为十六进制‘4’。

控制性文档
握奇智能

3. MAC的计算

MAC是使用命令的所有元素（包括命令头）产生的。MAC是命令数据域中最后一个数据元，它的长度为4个字节。

MAC的计算步骤如下:

第一步：终端向IC卡发出一个GET CHALLENGE命令，从IC卡取回4字节随机数。

第二步：将IC卡回送的4字节随机数后缀以‘00 00 00 00’，所得到的结果作为初始值。

第三步：按照顺序将以下数据连接在一起形成数据块:

- CLA，INS，P1，P2，Lc+4，DATA
- 必须置CLA的后半字节为十六进制‘4’。
- 在命令的数据域中（如果存在）包含明文或加密的数据。

（例: 如果要进行线路加密保护，加密后的数据块放在命令数据域中传输）

第四步：将该数据块分成8字节为单位的数据块，标号为D1，D2，D3等。最后的数据块有可能是1-8个字节。

第五步：如果最后的数据块长度是8字节的话，也必须在其后加上16进制数字‘80 00 00 00 00 00 00 00’，转到第六步。

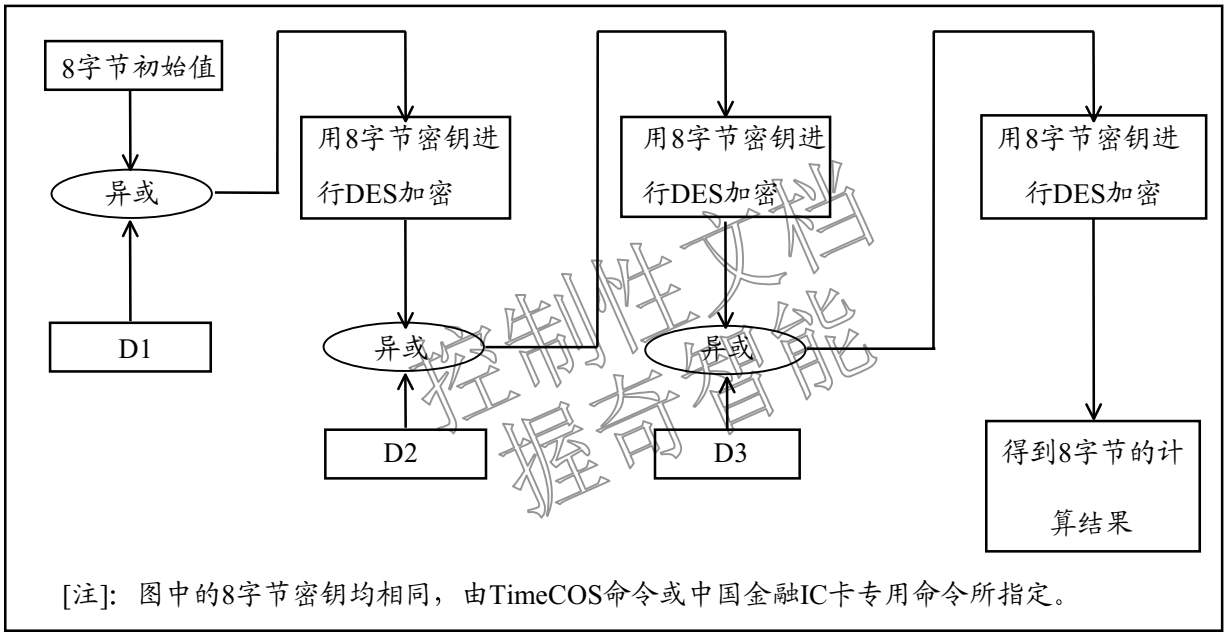
如果最后的数据块长度不足8字节，则在其后加上16进制数字‘80’，如果达到8字节长度，则转入第六步；否则在其后加上16进制数字‘00’直到长度达到8字节为止。

第六步：对这些数据块使用相应密钥进行加密。（密钥由TimeCOS命令或中国金融IC卡专用命令所指定）

如果该密钥长度为8字节，则依照图1的方式来产生MAC（根据在第三步中产生的数据块长度的不同，有可能在计算中会多于或少于三步）。

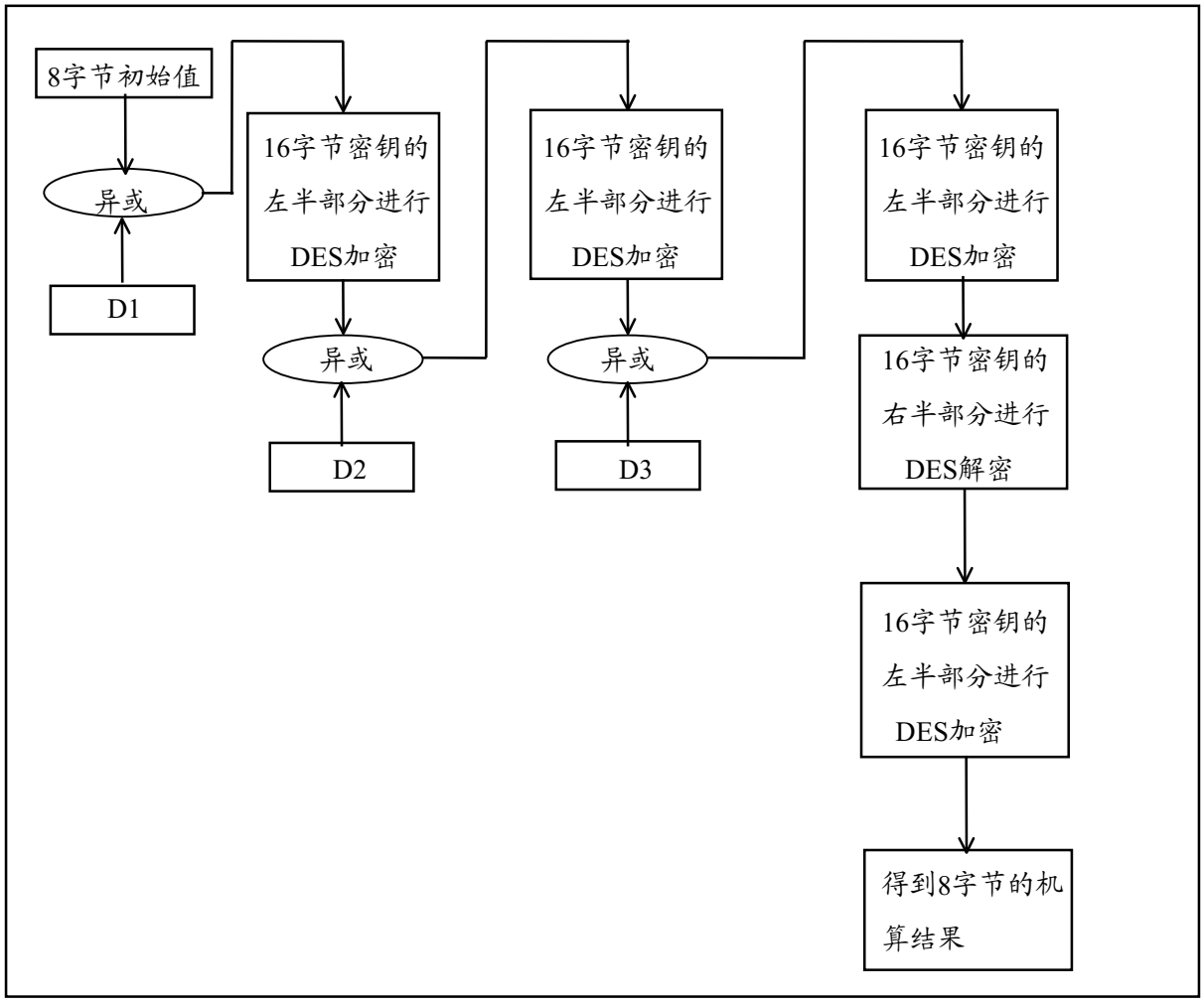
如果该密钥长度为16字节，则依照图2的方式来产生MAC（根据在第三步中产生的数据块长度的不同，有可能在计算中会多于或少于三步）。

第七步：最终得到是从计算结果左侧取得的4字节长度的MAC。



[注]：图中的8字节密钥均相同，由TimeCOS命令或中国金融IC卡专用命令所指定。

图1：用长度为8字节的密钥产生MAC的算法



[注]：图中的16字节密钥由TimeCOS命令或中国金融IC卡专用命令所指定。

控制性文档 握奇智能

图2：用长度为16字节的密钥产生MAC的算法

4. 数据加密/解密的计算

1). 数据加密计算步骤

第一步：用LD表示明文数据的长度，在明文数据前加上LD产生新的数据块。

第二步：将第一步中生成的数据块分解成8字节数据块，标号为D1，D2，D3，D4等等。最后一个数据块长度有可能不足8位。

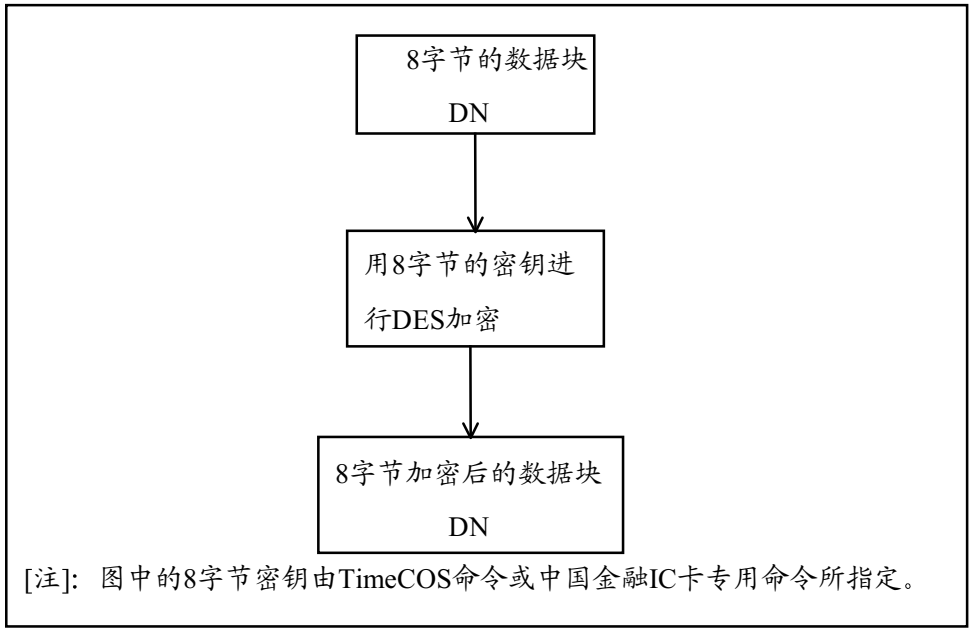
第三步：如果最后（或唯一）的数据块长度等于8字节，转入第四步；如果不足8字节，在右边添加16进制数字‘80’。如果长度已达8字节，转入第四步；否则，在其右边添加16进制数字‘00’直到长度达到8字节。

第四步：对每一个数据块使用相应密钥进行加密。（密钥由TimeCOS命令或中国金融IC卡专用命令所指定）

如果该密钥长度为8字节，则依照图1的方式来加密数据块。

如果该密钥长度为16字节，则依照图2的方式来加密数据块。

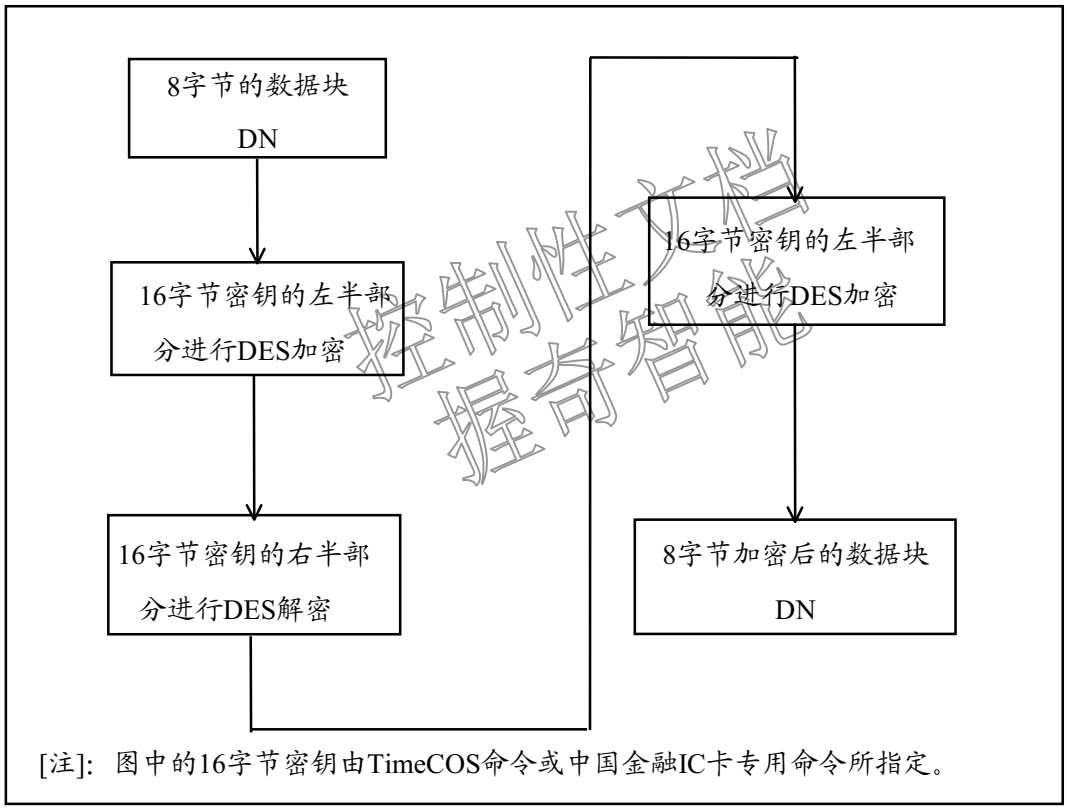
第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起（加密后的D1，加密后的D2，等等）。并将结果数据块插入到命令数据域。



[注]：图中的8字节密钥由TimeCOS命令或中国金融IC卡专用命令所指定。

图1：用长度为8字节的密钥进行数据加密的算法

控制性文档 指令智能



控制性文档
握奇智能

图2：用长度为16字节的密钥进行数据加密的算法

2). 数据解密计算:

第一步：将命令数据域块分解成8字节长的数据块，标号为D1，D2，D3，D4等等。

第二步：对每一个数据块使用与数据加密相同的密钥进行解密。（密钥由TimeCOS命令或中国金融IC卡专用命令所指定）

如果该密钥长度为8字节，则依照图3的方式来解密数据块。

如果该密钥长度为16字节，则依照图4的方式来解密数据块。

第三步：计算结束后，所有解密后的数据块依照顺序（解密后的D1，解密后的D2，等等）链接在一起。数据块由LD、明文数据、填充字符组成。

第四步：因为LD表示明文数据长度，因此，它被用来恢复明文数据。

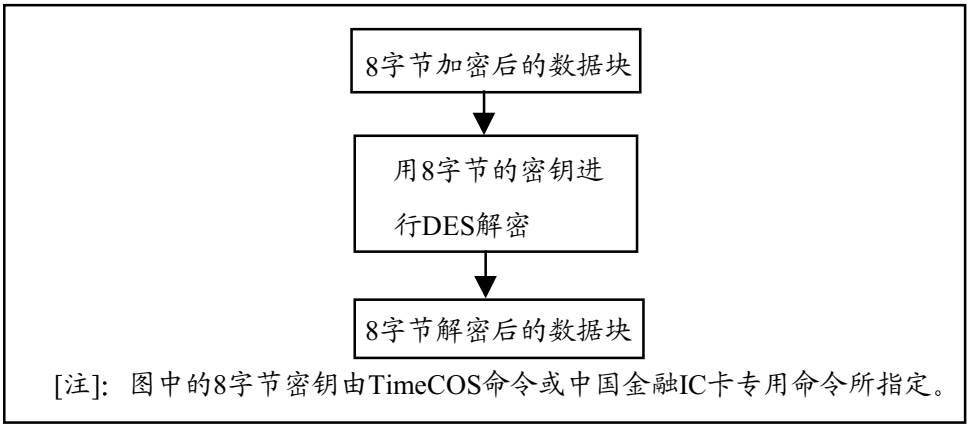
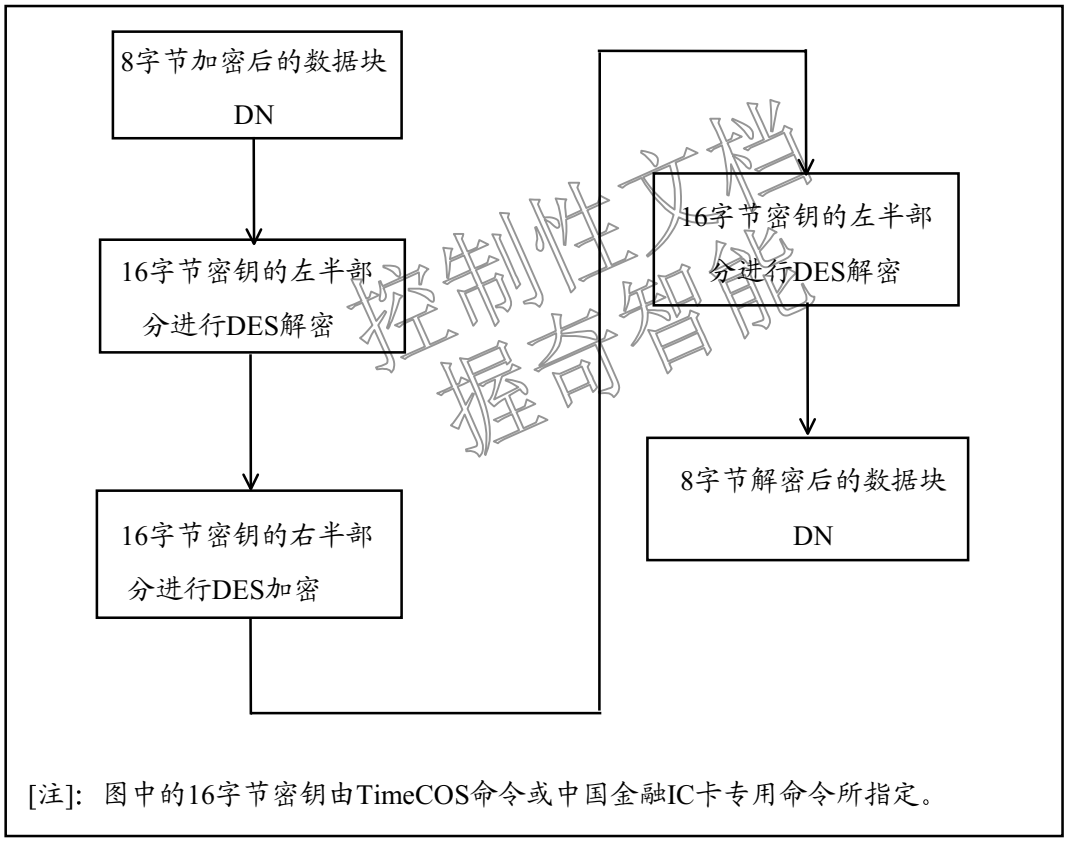


图3：用长度为8字节的密钥进行数据加密的算法



控制性文档
握奇智能

图4：用长度为16字节的密钥进行数据加密的算法

5. 安全报文传送的命令情况

CASE1：这种情况时，没有数据送到卡（Lc）中，也没有数据从卡中返回（Le）。

没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC

CLA的低半字节是‘4’表明支持第二种情况的安全报文传送技术。Lc为MAC的长度。

CASE2：这种情况时，命令中没有数据送到卡中，但有数据从卡中返回。

没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Le

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC	Le

CLA的低半字节是‘4’表明支持第二种情况的安全报文传送技术。Lc为MAC的长度。

CASE3: 这种情况时，命令中有数据传送到卡中，但没有数据从卡中返回。

没有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	命令数据

有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	命令数据	MAC

CLA的低半字节是‘4’表明支持第二种情况的安全报文传送技术。Lc为命令数据和MAC的长度。

CASE4: 这种情况时，在命令中有数据送到卡中，也有数据从卡中返回。

没有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	命令数据	Le

有安全报文传送要求的命令情况如下:

CLA	INS	P1	P2	Lc	命令数据	MAC	Le

CLA的低半字节是‘4’表明支持第二种情况的安全报文传送技术。Lc为命令数据和MAC的长度。

控制性文档 指令智能

附录一 TimeCOS 2.5金融IC卡应用举例

控制性文档
握奇智能

1). 主密钥内容

消费主密钥MPK_01: 70 E9 BE A6 97 72 3D F8 36 05 EB BC B7 C2 C7 C4

消费主密钥MPK_02: 6F 15 3B 35 A9 7E 1B 56 A1 F8 A3 CE 7A C5 DA E2

圈存主密钥MLK_01: D3 D6 E8 83 68 32 FD D4 70 6D 06 71 BB 8B D2 8B

圈存主密钥MLK_02: B1 17 DE 00 7E 79 E7 86 63 4B 73 A4 83 AE 97 46

TAC主密钥MTK: 13 8D 34 F8 4B 20 31 FF 47 9E 71 BE FF 10 7A 76

口令解锁主密钥MPUK: 07 C3 EA A0 99 7C E0 26 B8 62 9A 77 CC B5 AC 9A

口令重装主密钥MRPK: 48 39 6B 19 B5 E9 76 5F DA 25 EC 5C 39 40 58 A0

应用主密钥MAMK: 0F 6F F9 CC 72 20 43 71 09 39 16 F9 E8 BB F0 62

圈提主密钥MULK_01: E9 38 FD DA AE 9E 5C 8C E6 A1 37 B7 F1 62 E5 7E

圈提主密钥MULK_02: EF FA 77 3C 95 53 3A 03 71 BB A0 B2 D5 45 73 4A

修改透支限额主密钥MUK_01: 38 B4 BE 8A 7D 99 49 44 0A 86 8C 68 A6 45 92 16

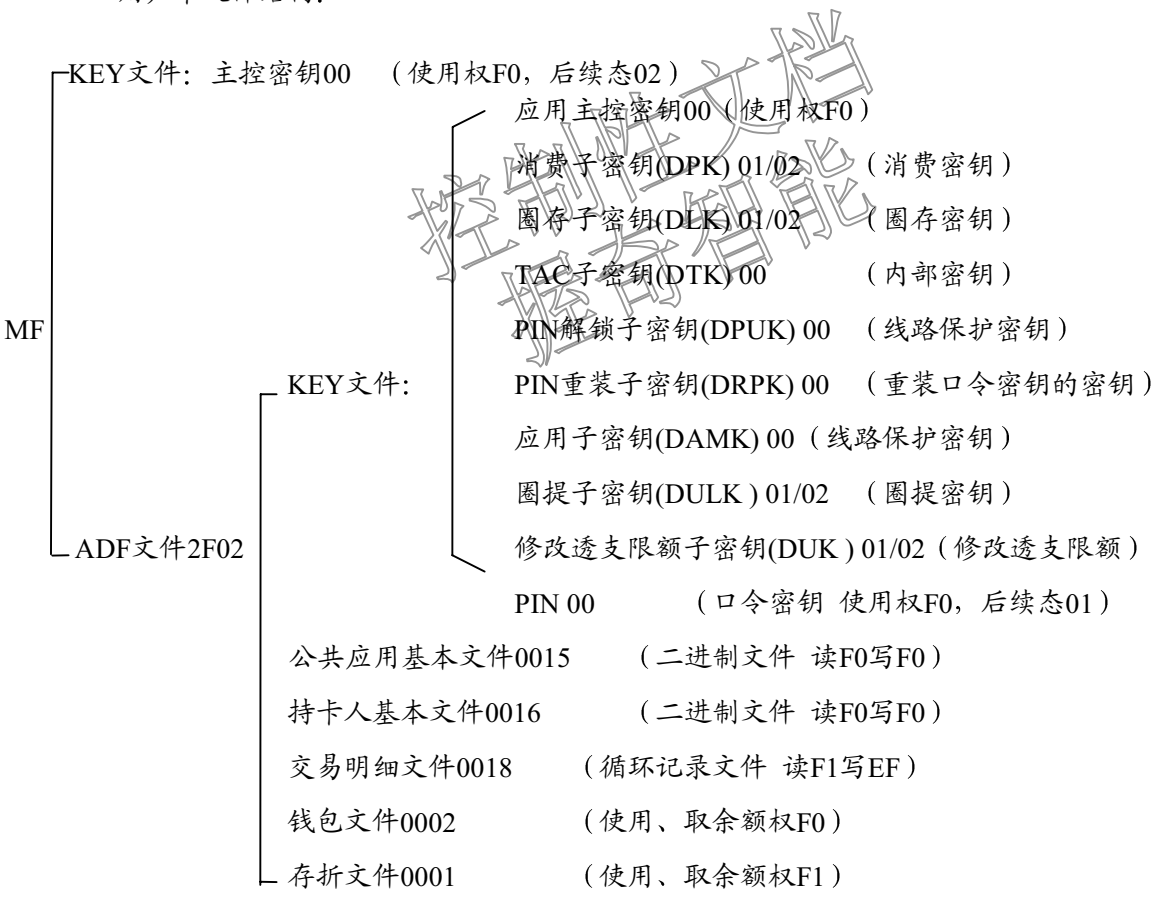
修改透支限额主密钥MUK_02: B0 6F C8 5C 75 22 F1 D8 3A 70 88 44 F3 3C AC FD

2). 消费SAM卡

消费SAM卡文件结构请参见《PSAM卡手册》。PSAM卡内有消费主密钥（算法级别为01）。

3). 用户卡

用户卡文件结构:



建立主文件: 80 E0 3F 00 0D 38 FF FF 22 22 01 FF FF FF FF FF FF FF

建立KEY文件: 80 E0 00 00 07 3F 00 1C FF EF FF FF

安装主控密钥: 80 D4 01 00 15 F9 F0 22 02 33 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

建立目录基本文件(DIR): 80 E0 00 01 07 2C 00 16 F0 22 FF FF

写目录基本文件: 00 DC 00 0A 15 70 13 61 11 4F 09 A0 00 00 00 03 86 98 07 01 50 04 50 42 4F 43

建立ADF: 80 E0 2F 02 11 38 02 F2 EF EF 95 FF FF A0 00 00 00 03 86 98 07 01

选择ADF: 00 A4 04 00 09 A0 00 00 00 03 86 98 07 01

建立KEY文件: 80 E0 00 00 07 3F 01 3C FF EF FF FF

应用主控密钥: 80 D4 01 00 15 F9 F0 22 02 33 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

安装DPK_01: 80 D4 01 01 15 3E F0 02 01 00 C8 F0 AA 97 65 F6 75 5F C1 78 4B B1 F3 55 9F 89

安装DPK_02: 80 D4 01 02 15 FE F0 02 01 00 C4 09 1B BA 14 DB 14 76 DE 20 28 2C BF 6B 4D CA

安装DLK_01: 80 D4 01 01 15 FF F0 02 01 00 AA B1 5E 01 5A D3 AD 2D C5 20 58 3A AD 85 62 C4

安装DLK_02: 80 D4 01 02 15 FF F0 02 01 00 F0 4E 39 1B AC CD EC E9 90 9E AD 78 92 15 12 17

安装DTK: 80 D4 01 00 15 F4 F0 02 01 00 7D 4C C5 20 17 58 A9 60 64 53 61 DF C2 93 67 4E

安装DPUK: 80 D4 01 00 15 F7 F0 02 FF 33 EC 7C B7 3F A4 56 43 5C 79 B4 43 11 FE EF 45 B1

拉制性文档 指南智能

安装DRPK:　80 D4 01 00 15 F8 F0 02 FF 33 BD 98 E4 AA 4E 65 61 58 69 B8 C3 BA 5C ED FA 9F

安装DAMK: 80 D4 01 00 15 F6 F0 02 FF 33 14 0D AE 09 16 A9 B1 6B 5C 64 F2 2F 6C E5 37 8F

装DULK_01: 80 D4 01 01 15 FD F0 02 01 00 3C 3D 46 BD 7D 7A 61 98 98 5D 8F 45 4B 12 BB CF

装DULK_02: 80 D4 01 02 15 FD F0 02 01 00 A3 86 FA DE DE D1 54 1C EE 82 BA D0 BD 68 8F C5

安装DUK_01: 80 D4 01 01 15 FC F0 02 01 00 76 71 A1 04 11 82 04 48 D7 FD F4 24 2C 4A FC AD

安装DUK_02: 80 D4 01 02 15 FC F0 02 01 00 33 11 C4 42 A3 27 5B DB F3 F7 50 40 D0 FE C7 B0

安装PIN:　　80 D4 01 00 0B 3A F0 EF 01 33 12 34 FF FF FF FF

建立公共应用基本文件: 80 E0 00 15 07 A8 00 1E F0 F0 FF FF

写基本应用文件: 00 D6 95 00 1E 11 11 22 22 33 33 00 06 03 01 00 06 19 98 08 17 00 00 00 30 19 98 08 15 19 98 12 15 55 66

建立持卡人基本文件:　　80 E0 00 16 07 A8 00 27 F0 F0 FF FF

写持卡人基本应用文件: 00 D6 96 00 27 00 00 53 41 4D 50 4C 45 20 43 41 52 44 20 41 44 46 31 00 00 00 00 31 31 30 31 30 32 39 38 31 32 31 38 30 30 31 30 05

建立交易明细文件: 80 E0 00 18 07 2E 0B 17 F1 EF FF FF

建立电子存折文件: 80 E0 00 01 07 2F 02 08 F1 00 FF 18

建立电子钱包文件: 80 E0 00 02 07 2F 02 08 F0 00 FF 18

4). 子密钥推导方法

以生成16字节的消费子密钥为例，在银行应用目录下，子密钥的生成均可参考此例。

消费子密钥(DPK)左半部分的推导方法

1. 将本张用户卡的应用序列号的最右8个字节作为输入数据。
2. 将16个字节的消费主密钥(MPK)作为加密密钥。
3. 用消费主密钥(MPK)对输入数据进行Triple DES运算。

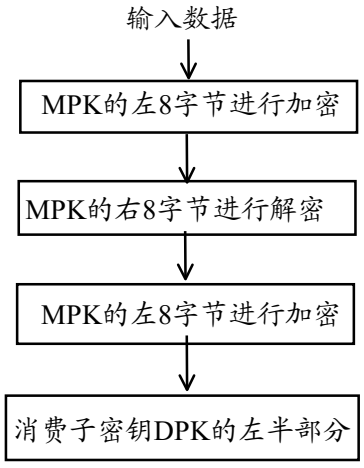


图1: 推导16字节的消费子密钥的左半部分

智能卡技术规范 指南

消费子密钥(DPK)右半部分的推导方法

1. 将本张用户卡的应用序列号的最右8个字节的求反作为输入数据。
2. 将16个字节的消费主密钥(MPK)作为加密密钥。

5). 电子存折/电子钱包应用的基本数据文件

文件标识符	‘0015’
文件类型	‘A8’（线路保护的二进制文件）
文件主体空间	‘1E’
读权限	‘F0’（自由读取）
写权限	‘F0’（写二进制时必须使用DAMK进行线路保护，如连续三次执行此命令失败，IC卡回送‘9303’即应用永久锁定）

字节	数据元	长度
1-8	发卡方标识	8
9	应用类型标识	1
10	应用版本	1
11-20	应用序列号	10
21-24	应用启动日期	4
25-28	应用有效日期	4
29-30	发卡方自定义文件控制信息数据	2

表1：电子存折和电子钱包应用的公共应用基本数据文件

文件标识符	‘0016’
文件类型	‘A8’（线路保护的二进制文件）
文件主体空间	‘27’
读权限	‘F0’（自由读取）
写权限	‘F0’（写二进制时必须使用DAMK进行线路保护，如连续三次执行此命令失败，IC卡回送‘9303’即应用永久锁定）

字节	数据元	长度
1	卡类型标识	1
2	本行职工标识	1

控制性文档 指南智能

3-22	持卡人姓名	20
23-38	持卡人证件号码	16
39	持卡人证件类型	1

表2：电子存折和电子钱包应用的持卡人基本数据文件

文件标识符	‘0018’
文件类型	‘2E’（循环文件）
记录个数	‘0A’（该循环文件必须能够容纳至少十条消费、取现、圈存、圈提交易 记录）
记录长度	‘17’
读权限	‘F1’（必须先验证口令）
写权限	‘EF’（交易明细由IC卡维护，不允许外部对其修改）

字节	数据元	长度
1-2	电子存折/电子钱包联机或脱机交易序号	2
3-5	透支限额	3
6-9	交易金额	4
10	交易类型标识	1
11-16	终端机编号	6
17-20	交易日期	4
21-23	交易时间	3

表3：电子存折和电子钱包应用的交易明细文件

控制性文档 捷点智能

附录二 TimeCOS 2.5安全管理

TimeCOS在卡片生命周期的安全控制过程:

芯片制造 ⟶ 模块封装 ⟶ 卡片制造 ⟶ 卡片封装 ⟶ 卡片初始化 ⟶

安装发行密钥 ⟶ 卡片个人化 ⟶ 卡片应用

控制性文档
握奇智能

1. 芯片制造是将TimeCOS的程序代码掩膜到芯片上。

   为保证芯片运输过程的安全，在芯片制造时，半导体厂商设定了7字节的传输代码。

   如用户无特殊要求，8字节的传输代码为8个字节的FF。在建立MF时，若传输代码错误，则内部错误计数器加一，若错误次数超过7次，则芯片自动锁死不可再用。

2. 模块封装是将已制造好的芯片安装在有8个触点的印刷电路板上。

   芯片制造商没有卡片初始化等参数，无法打开卡片。

3. 卡片制造与封装是将封装好的主模块嵌入塑料卡中。

4. 卡片初始化即设置TimeCOS参数。

   在卡片初始化之前，只能使用卡片初始化指令。

5. 安装发行密钥即创建MF，并在MF下建立一个外部认证的发行密钥。

   在芯片运输到卡片制造商后，卡片制造商将测试合格的芯片制成卡片且装入发行密钥后，可运送给发行商。

   为了保证卡片运输过程的安全，发行商可将自定义的发行主密钥提供给卡片制造商用以生成发行密钥。

   卡片制造商将卡片复位时得到的历史字节的后8个字节即8字节卡序号作为输入数据，用发行主密钥对其进行加密生成发行密钥并写入卡片中。(发行密钥生成方法见附1.4)

   由于每张卡片具有唯一的卡序号，所以每张卡片中的发行密钥也具有唯一性。

[注]：在建立MF之前，只能使用卡片初始化指令；在建立MF之后，只能使用除卡片初始化指令或建立MF指令外的其它指令。

6. 卡片个人化即建立应用文件并写入持卡人资料。

发行商收到卡片后，发行商用发行密钥对卡片进行外部认证，认证成功之后即可修改发行密钥或擦除MF。若连续三次认证发行密钥失败则卡片自动锁死不可再用。

说明：通过上述步骤的卡片在发行阶段，不用创建MF，MF在卡片制造时已根据芯片类型按最大空间创建完MF，擦除权限和建立权限缺省为22H（可根据发行商要求而定），MF下建立了一个KEY文件，装有一个Triple DES密钥。

控制性文档
振奇智能

7. 卡片应用即持卡人使用发行好的卡片到应用系统中应用。

附录三 TimeCOS技术性能指标

控制性文档
指令智能

一. 硬件技术性能参数

TimeCOS已经在很多种类型的芯片上实现，以下是部分芯片的硬件性能参数。随着技术的发展日新月异，这些指标将有变动，对于这些变动，本公司不再另行通知。

技术指标	SLE44系列芯片	SLE66系列芯片	三星KS88SC92008	飞利浦P83C862
微处理器	8位保密控制器	8/16位保密控制器	8位保密控制器	8位保密控制器
程序空间ROM	17K	32K	32K	20K
RAM	256字节	256字节	256字节	256字节
EEPROM	512字节/1K/2K/4K/8K/16K			
时钟频率	1～5MHZ可选，缺省为3.57MHZ			
EEPROM寿命	500,000次			
擦写时间	擦写1/2/4/8/16字节时需5.28/5.31/5.38/5.52/5.8毫秒			
数据保存时间	10年			
工作电压	2.7～5.5 V,缺省为5 V			
工作电流	小于10 mA			
省电模式	当TimeCOS等待接收命令时处于休眠状态，最大电流100微安			
温度	-25～+70摄氏度			
通讯速率	支持9600bps,19200bps,38400bps,76800bps可选,缺省为9600bps			
通讯协议	支持T = 0,T = 1可选,缺省为T = 1			
APDU长度	APDU的最大长度为183字节			

二. TimeCOS技术性能参数

以下列出TimeCOS在执行某些指令或运算是所需的时间参数，供参考，这些参数的测试条件如无特别注明为：接触模式、工作时钟3.57MHz、T＝0协议、波特率9600bps。参数本身如无特别注明只包括命令或运算的执行时间，而不包括通讯时间。时间单位为ms。

技术指标	SLE44系列芯片	SLE66系列芯片	三星KS88SC92008	飞利浦P83C864
TripleDES时间	37	16	0.2	0.2
SHA算法时间	147ms/64 Bytes	73ms/64 Bytes		
RSA签名时间		268		
RSA认证时间		18		
RSA加密时间		21		
RSA解密时间		268		
FAC签名时间	95ms/32 Bytes			
以下为PBOC指令执行时间				
圈存（存折）	130	85	49	44
圈提	125	82	46	56
修改透支限额	127	81	46	39
消费（存折）	178	103	61	58
消费（钱包）	146	91	58	55
解锁应用	58	39	31	29
应用锁定	53	35	25	24
重装PIN	46	34	32	31
解锁PIN	106	62	36	31

控制性文档 握奇智能